Field Manual
No. 19-30

Headquarters
Department of the Army
Washington, D.C. 1 March 1979



*This publication supersedes FM 19-30, 3 November 1971, including all changes.

You, the user of this manual, are the most important element in keeping this publication current and viable. You are encouraged to submit any comments or recommendations pertinent to this field manual. Comments should be keyed to the specific page and line of the text in which you feel an improverment is needed. You should provide reasons for each comment made to insure complete understanding and evaluation Make your comments on DA Form 2028 (Recommended Changes to Publications) and forward to the Commandant, USAMPS/TC, ATTN: ATZN-TDP-C, Fort McClellan, AL 36205. Every comment will be considered.

The word "he" in this publication is intended to include both the masculine and feminine genders and exception to this will be noted.

1 MARCH 1979

By Order of the Secretary of the Army:

BERNARD W. ROGERS
General, United States Army
Chief of Staff

Official:

J. C. PENNINGTON
Major General, United States Army
The Adjutant General

DISTRIBUTION:

Active Army, USAR and ARNG: To be distributed in accordance with DA Form 12-11A, Requirements for Physical Security (Qty rqr block no. 142).

Additional copies can be requisitioned from the US Army Adjutant General Publications Center, 2800 Eastern Boulevard, Baltimore, MD 21220.

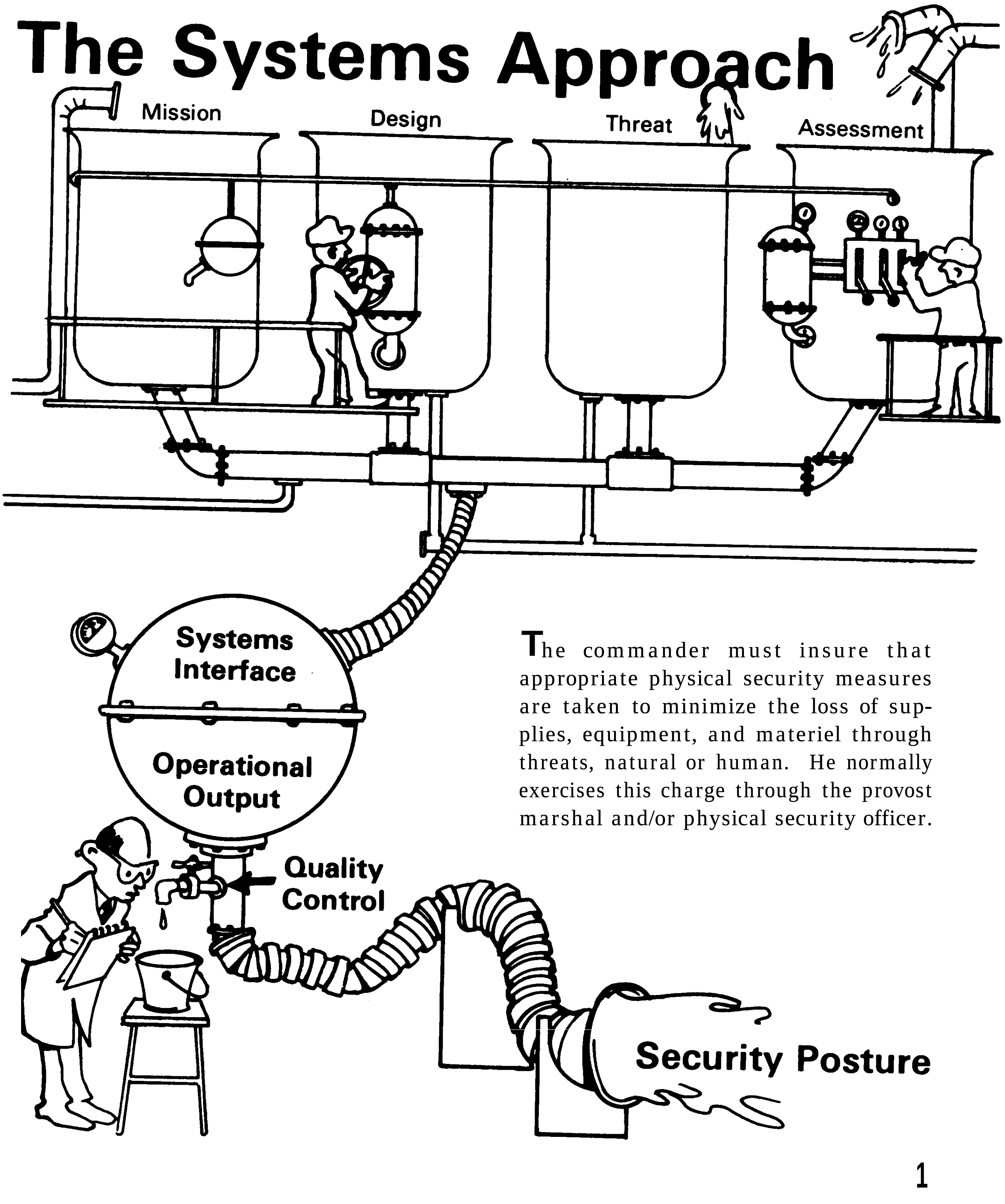
U. S. GOVERNMENT PRINTING OFFICE : 1994 - 153-846

Physical Security

TABLE OF CONTENTS

Chapter 1

The Systems Approach



The commander must insure that appropriate physical security measures are taken to minimize the loss of supplies, equipment, and materiel through threats, natural or human. He normally exercises this charge through the provost marshal and/or physical security officer.

1-1 System Design

You should formulate and implement your basic physical security design from a total system approach. It should be organized in depth and contain mutually supporting elements and be coordinated to prevent gap or overlap in responsibilities and performance.

a. Total system approach is based on:

(1) Thoughtful and continuing analysis of existing protective measures.

(2) Determination of the possibility of interference with the operational capabilities of the installation or facility from any or all sources.

(3) Careful evaluation of the measures necessary and practicable that maintain security at a desired level.

(4) Tailored to the needs and local conditions of each installation or activity.

b. Mutually supporting elements include:

(1) Physical perimeter barrier(s).

(2) Clear zones.

(3) Protective lighting.

(4) Entry control facilities.

(5) Detection, including the use of sensors and assessment systems.

(6) Warning systems.

(7) Perimeter defensive positions, if appropriate.

> **Note:** Selection and use of **means beyond minimum requirements:**
>
> ■ Established by command directives.
> ■ Coordination and cooperation between physical security officers and facilities engineers is a necessity.
> ■ Wherever threat indicates need for increased security.

1-2 Design Considerations

a. Available resources must be used in the most efficient manner to achieve adequate protection for an entire installation.

b. Emphasis goes to the **operational requirements** of the installation in determining the type and extent of physical protection. The physical security manager should consider the following pertinent factors in the indicated sequence.

(1) Mission assignment— importance of the installation or unit to the mission of the Army.

(2) The area to be protected, including the nature and arrangement of the activity; classification of information, data, activities; the number of personnel involved; monetary and/or strategic value of materiel located therein; or other important features inherent to the problem, such as existing threats, either natural or human.

(3) Criticality and vulnerability of information, materiel and personnel.

(4) Integration of operating, maintenance, and other requirements.

(5) Environment, such as political and economical aspects, legal considerations, terrain, weather, climate, etc.

(6) Feasibility, effectiveness, and desirability of various possible methods of providing adequate protection.

(7) Costs of materiel and equipment to be installed as well as availability of finds to provide at least minimum protection for all critical areas and activities This minimum may be less than the desirable degree of physical protection; therefore, the program must be flexible so that refinements can be added as additional resources become available.

(8) Possible changes in operation, such as expansion, relocation and retrenchment. Coordination must be maintained with appropriate staff offices so that changes may be projected as far in advance as possible, and necessary supplemental personnel and/or funds can be requested.

c. Changes in mission and activities of an installation or activity may also require adjustments in security. **Physical security planning and programing must be a continuing process** if security managers are to provide the best protection possible.

d. All security measures should be employed so that they complement and supplement each other. Lack of integration of security measures may result in a waste of money, equipment, and manpower. But more important, the security of an installation may be placed in jeopardy. By the considerations outlined, a sound physical security program should evolve.

e. The **formulating procedure** is sound whether it is applied to changes on existing installation or the construction of a new facility.

1-3 Assessment Of Security Posture

The degree of protection desired on any installation is predicated upon an analysis of two factors-criticality and vulnerability.

a. Resource Criticality

(1) Determination

(a) Importance to the national defense structure.
(b) Effect of its partial or complete loss.

(2) Evaluation

(a) Installation. High criticality-great effect on national defense structure.
(b) Command/activity. High criticality—partial or complete loss—immediate and serious impact to perform its mission for a considerable period of time.

b. Resource Vulnerability

(1) Determination

(a) Susceptibility to threats that result in damage, loss, destruction or disruption.
(b) Type Of installation or activity involved, industrial or other processes performed, physical layout and construction.

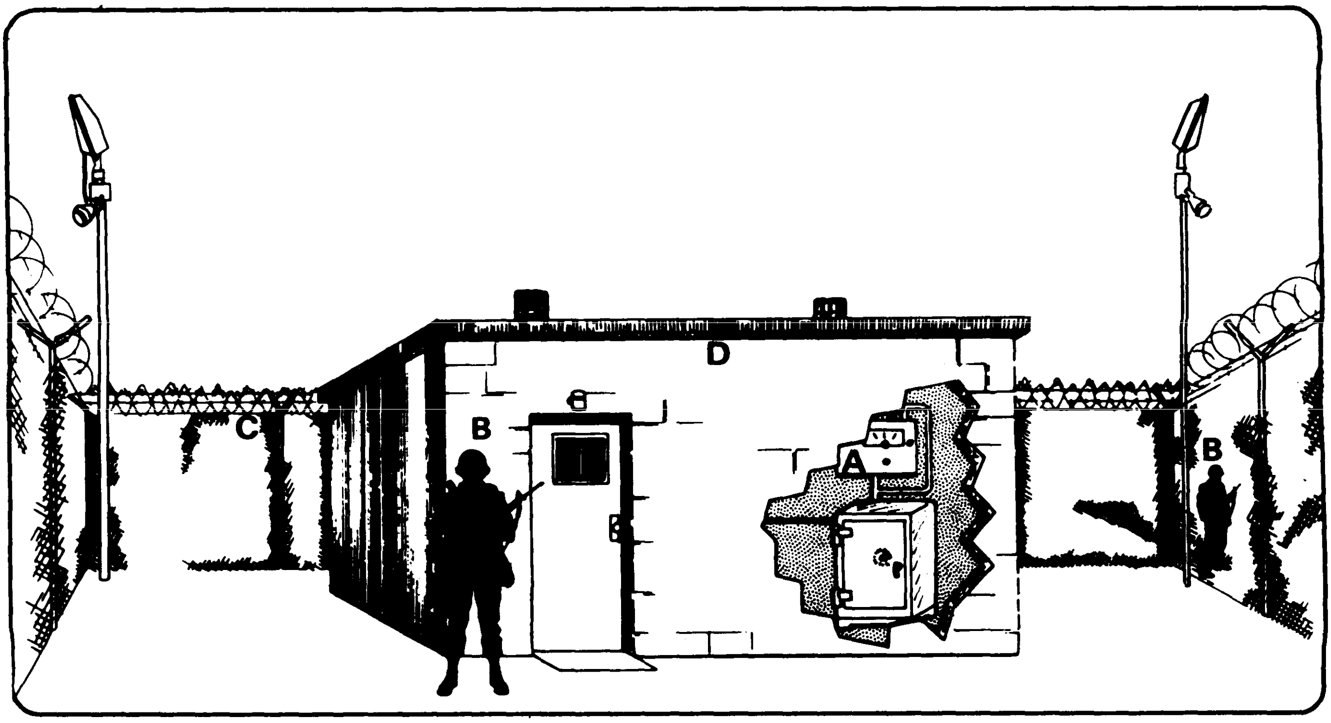
(2) Evaluation

(a) High vulnerability—one or more threats easily causing sufficient loss, damage, or destruction to affect the mission of the whole installation or its subordinate commands/activities.
(b) Decreased vulnerability—existing threats not likely to cause interference with the mission.
(c) It should be noted that cost of

protective measures in terms of equip ment and manpower may not allow for optimum security for the entire installation. Also, determination of security priority based on criticality and vulnerability is essential to proper allocation of resources.

c. Security in depth (guards, physical barriers, and systems) is always the goal of those individuals responsible for the security of an installation or activity. No object is so well protected that it cannot be stolen, damaged, destroyed, or compromised. Therefore, access must be made so difficult that an intruder will be deterred from committing a criminal act or will be detected and apprehended before he can successfully complete the criminal act. **Accumulated delay time for the intruder must be built into a system for protection in depth.** This protection results from the security in-depth ring (see figure 1).

d. Physical security is only part of the overall defense plan of an installation. It does not include dispersion of facilities, continuity of operations, civil defense structures, construction specifications, or plans formulated to cope with natural or human threats that happen. The formulating process must allow for the integration of all these measures.



LEGEND

A IDS
B Guards
C Barrier
D Building (barrier)

Figure 1—Security in-depth ring.

Security Threats

Security threats are acts or conditions that may result in the compromise of information; loss of life; damage, loss, or destruction of property; or disruption of the mission of the installation or facility. Before the physical security manager can develop an effective security program, he must determine the possibility of interference with the operational capabilities of the installation or facility from any and all sources. Recognition of all risks is mandatory if he is to make recommendations for physical security measures to control or eliminate them. The severit y of security threats depends on such variables as the type of installation or facility involved, mission or processes performed, physical layout, and construction. The geographical location, the enemy situation, and the existing state of law and order are most important factors.

1-4 Definition

a. Security threats are acts or conditions, which include human threats, that may result in:

(1) Disruption of the installation or facility.

(2) Damage, loss or destruction of property.

(3) Personal injury or loss of life.

(4) Compromise of defense information.

b. Threat severity depends on such variables as:

(1) Type of installation or facility.

(2) Mission or processes performed.

(3) Physical layout and construction.

(4) Geographical location.

(5) Stability of the situation.

(6) Existing state of law and order.

(7) Protection measures in effect.

1-5 Categories

Security threats are classified as either natural or human.

a. Natural Threats

(1) Usually the consequence of natural phenomena.

(2) Normally not preventable by physical security measures.

(3) May greatly affect security operations in one or more of these ways.

(a) Require an increase in protective measures.
(b) May reduce the effectiveness of existing security measures by such occurrences as:

- Collapsed perimeter fences.
- Inoperable protective lighting.
- Damaged patrol vehicles.
- Poor visibility.

Examples of natural threats are:

Floods— flooding of the installation with resulting property damage, destruction of perimeter barriers and short circuiting of intrusion detection systems. Heavy rains or snowfalls, even though they do not result in floods, may cause some of the same damages.

Storms— high winds or rain causing nuisance alarms and short circuiting in IDS, and limiting visibility of security personnel.

Earthquakes— causing nuisance alarms, possible fires from broken gas mains, buildings weakening and falling down.

Winds— disrupting power lines, setting off nuisance alarms, causing safety hazards with flying debris.

Snow and Ice— blocking patrol roads, increasing response time to alarms, and freezing of locks and alarm mechanisms.

Fires— damage/destruction of perimeter barriers or buildings.

Fog— causing reduced visibility for security forces and increased response time to alarms and may require additional security personnel.

b. Human Threats

These threats are the result of a state of mind, attitude, weakness, or character trait on the part of one or more persons. They include acts of commission or omission—overt and covert—which could disrupt or destroy the operation or mission of an installation or facility.

Examples of human threats are:

❑ Pilferage (appendix A).
❑ Sabotage (appendix B).
❑ Espionage (appendix C).
❑ Bombing (appendix D).
❑ Pilferage in Consumer Outlets (appendix A).
❑ Attacks on Key Persons (chapter 14).
❑ Carelessness and accidents in performance of official duties.
❑ Disaffection and disloyalty of employees.
❑ Safety hazards from equipment malfunction.
❑ Human Intelligence Threat (HUMINT).

1-6 Risk Analysis

This process is invaluable to the security manager in establishing priorities of protection of assets. Basically, it consists of

a. Identifying items and functions in terms of:

(1) Total replacement

(2) Temporary replacement

(3) Unrecoverable costs

(4) Allied and related costs.

b. Conducting a hazards and vulnerability study of personnel, facilities, items, and functions.

c. Conducting a probability of occurrence assessment through indicators, such as:

(1) Documented records

(2) Insurance claims or adjustments

(3) Weather, etc.

d. Establishing a range of losses based on experience involving specific items (minimum to maximum in terms of dollar value), and assessing the losses over a 3-5 year period.

e. Correlating the degree of loss experienced with the ranges of losses or functions.

f. Comparing the low against high elements of ranges for all items and functions; then averaging weight against risk value in terms of criticality (Defense Industrial Security Institute, DSA).

1-7 Evaluation of Risks

The actual degree of risk involved depends on two factors:

■ Probability of adverse effects occurring as a direct result of the threat(s).

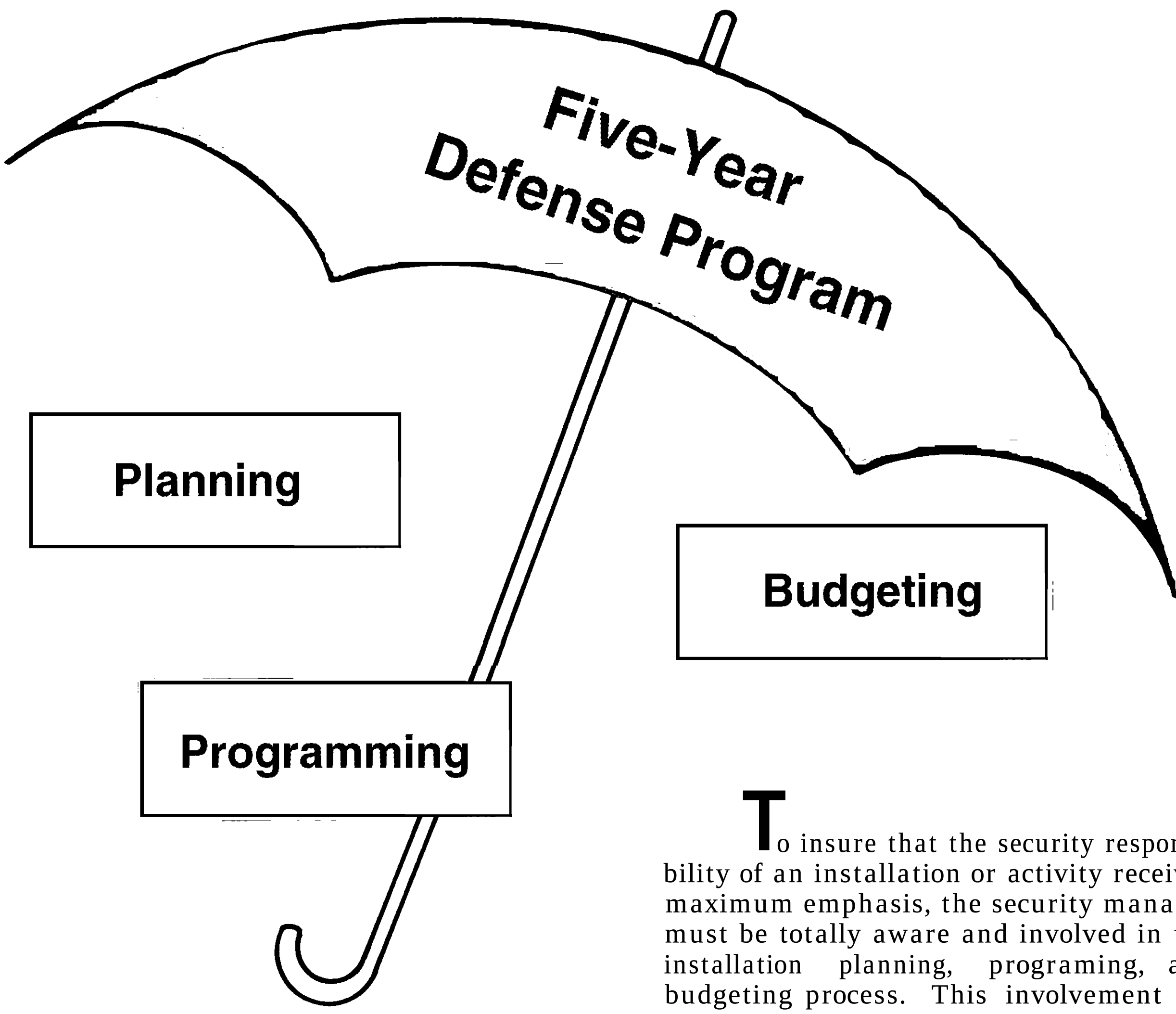
■ Extent to which the installation or activity will be affected by the threat(s).

Security threats significantly impact on a physical security program by requiring the incorporation of the following considerations:

❑ All determinable threats.
❑ Continuing activity beginning in peacetime and expanding to meet the particularities of formal hostilities.
❑ Coordination and integration with other protective programs, such as crime prevention and safety.

Chapter 2

Planning, Programing, and Budgeting



To insure that the security responsibility of an installation or activity receives maximum emphasis, the security manager must be totally aware and involved in the installation planning, programing, and budgeting process. This involvement includes preparation of manpower reports and appropriate submissions.

Planning for the security defense of an installation must remain constant, practical, flexible to the mission and certainly responsive to the needs of the commander. Only through adequate planning can we provide an effective counter response to security threats-as outlined in chapter 1.

2-1 Planning Basis

a. Implementation of Department of the Army (DA) policy, AR 190-13, and those supplemental directives by installation and higher commanders is imperative to having a sound security, program.

b. The following must be considered when planning security measures for an installation:

(1) Mission.

(2) Vulnerability.

(3) Impact on operations.

(4) Budget limitations.

(5) Personnel and equipment limitations.

2-2 Objectives

To be effective, planning must involve a phased approach, be flexible in incorporating changes, and have clearly defined courses of actions. It must be concerned with realistic protection in depth and be based on:

a. Relative standards.
b. Personnel, materiel and equipment available.
c. Probability of the most serious incident.
d. Implementation in the interest of continuity of all security operations.

2-3 Pre-operational Phase (Estimate)

a. Sound prior estimates of the security operational situation will reap big dividends when planning is ongoing. As a minimum, the preoperational estimate should be concerned, with the latest

(1) Security Analysis and Vulnerability Estimate (SAVE)

(2) Security Vulnerability Assessment (SVA)

(3) Operational Security (OPSEC).

b. The estimate must involve determination of all available resources and acts as the basis for developing a sound security plan.

c. The estimate should entail maximum use of existing organizational structures, supervisors, materiel and equipment, and available technical skills.

(1) Identification of unknown factors and limitations.

(2) Identification of the necessary augmentation of personnel and equipment to support the operational phase.

2-4 Operational Phase

Planning for the operational phase must be all inclusive. It involves training programs concerning duties and responsibilities prior to, during, and after the operational phase. As a minimum, this phase should cover:

a. Employment of assigned and attached personnel.

b. Serviceable equipment.

2-5 Awareness Phase

To insure that the operational phase is sound and that the plan is workable and practical, all personnel must be aware of their duties and responsibilities. Contents of the plan must dictate requirements and courses of action to include the interface of security personnel.

Extracts of the plan must be provided to key personnel and supervisors to insure areas of responsibility are executed. Also, supervisors must brief their personnel on appropriate duties and responsibilities, and monitor their actions to insure a successful plan exists.

2-6 Development

Developing a sound security plan must involve an integrated approach as to who, what, when, where and how. Specifically, the development should be in accordance with appendix F of this manual.

2-7 Evaluation

a. This is an important element of any plan to insure the plan's overall appropriateness and workability. Sound evaluation procedures will identify plan deficiencies and allow for necessary corrections and adjustments.

b. Evaluation of the plan will actually acquaint personnel with their duties and responsibilities as well as the mechanics of the plan.

c. The methods of evaluation should include:

(1) Testing techniques in which all portions of the plan are exercised individually and collectively.

(2) Testing conditions which are as close as possible to real world conditions and which simulate security threats as appropriate.

(3) Quality control through selecting evaluators who can provide a complete critique of the workability and appropriateness of the plan. Evaluators should be instructed to place special emphasis on personnel actions, both individually and collectively as a team, when weaknesses in training are evident. The evaluator should make note. An essential element of the evaluation is the feedback by evaulators. This feedback acts as a procedure for revising and modifying the plan. Revision should be immediate and all personnel must be made aware of the changes.

(4) Evaluation Frequency:

(a) The plan must be evaluated at irregular intervals based on published directives and as deemed necessary by . the responsible commander.

(b) Mechanics involving development of a security plan should consider the processes outlined in figure 2 and incorporate the data set forth in appendix F.

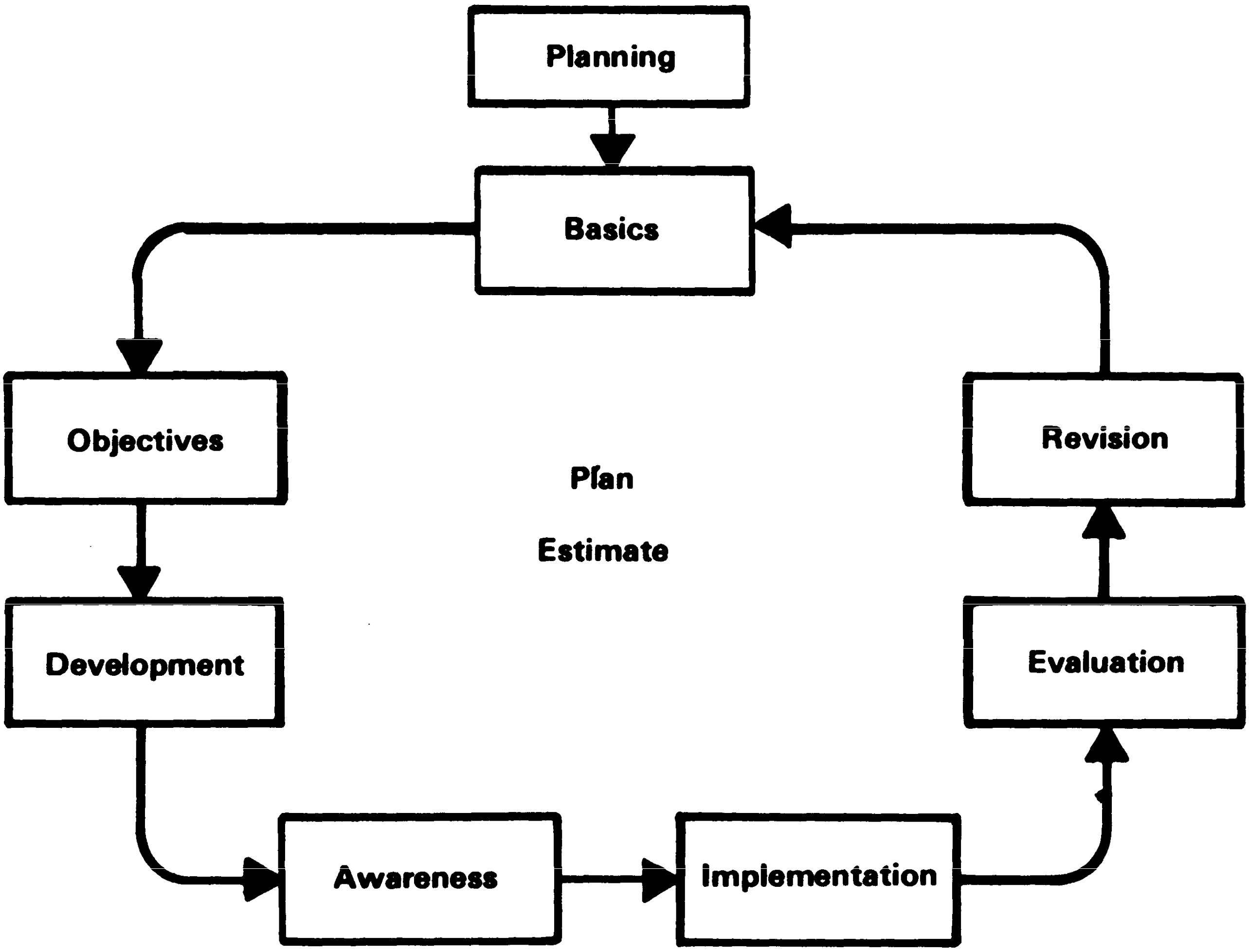


Figure 2—Process steps in effective planning.

Programing and Budgeting

Section II

As the Army continues to mature in terms of complexity and sophistication of weapons and equipment, the management of Army resources becomes an increasing responsibility. Inherent to this responsibility is the need for advanced security equipment, more and better trained security personnel, both civilian and military. Therefore, the security manager must be knowledgeable in resource management.

It is essential, in the management of installation security measures and requirements, that the security manager knows the working relationships and necessary requirements involving budget formulation and execution of the following:

- ❑ Command Budget and Manpower Guidance (BMG).
- ❑ Program Budget Advisory Committee (PBAC).
- ❑ Command Operating Budget Estimate (COBE).
- ❑ Major Activity Directors (MAD).
- ❑ Budget Requests.
- ❑ Manpower Procedures.
- ❑ Justification for Additional Security Personnel and Equipment.

2-8 Budget and Manpower Guidance (BMG)

a. Budget and manpower guidance is generated at Headquarters, DA, to insure that Army responsibilities spelled out in the FYDP are passed down to major commands and agencies.

b. Through this guidance DA spells out for each major command and agency precisely what will be required and what limitations are to be imposed. Based on this guidance, major commands and agencies update their 5-year programs and generate budget estimates for the budget year. The document each command or agency develops is its budget and manpower guidance (BMG).

2-9 BMG Objectives

a. The BMG is the basis for planning, programing and budgeting for all assigned missions, objectives and workloads.

b. This document provides higher headquarter's approval for use of all assigned resources for a specific period. The document is an extract from the Army portion of the FYDP of those resources that have been contemplated for allocation and contains goals and workloads that such resources are designed to support.

2-10 Concepts

a. Major command/agency 5-year programs, written in terms of appropriations, budget programs, and elements of expense, are detailed statements of the planned application of the resources (based on DA guidance) to accomplish assigned missions, goals, and workloads of the command for 5 years.

b. DA's budget and manpower guidance for major commands and agencies does not constitute authority to obligate finds. Rather, it is guidance to which recipients respond with their budget estimates and, finally their command operating budget estimates (COBE). This guidance document from Headquarters, DA, is formally updated three times a year.

c. Each successive headquarters translates the guidance it receives from above into expanded guidance for its subordinate commands. This action carries guidance from Headquarters, DA, down to the operating levels where, in response, the COBE is generated.

2-11 Command Operatin Budget Estimate (COBE)

a. The command operating budget estimate (COBE) is the field commander's estimate of resource requirements for the approaching fiscal year and an estimate of the following fiscal year based on advanced budget plans. Headquarters, DA, will advise

field commands of their approved operating budgets through four interrelated actions.

(1) June update of program and budget guidance.

(2) DA issuance of the resources guidance.

(3) Issuance of approved operating budget.

(4) Command operating budget markup.

b. Missions are assigned and resources are allocated to the installation commander in the command operating program of higher headquarters. The allocation is expressed in terms of the Army management structure, AR 37-100 (basic fiscal code), and AR 37-100-XX (FY fiscal code). Within this broad framework the installation commander develops a more detailed description of activities to be performed during the year. When approved, the COBE becomes the plan of action for executors of the program.

c. The COBE is a command, agency or installation plan of action for a specific fiscal year covering the activities for which it was responsible.

2-12 Purpose of COBE

a. To record in one place the activities to be conducted for a given year and the resources for their support. These are the activities necessary to achieve objectives assigned by higher authority based on guidance extracted from the Army portion of the FYDP.

(1) Identify that portion of the budget to be accomplished by each subordinate element in terms of objectives, policies, priorities, and resources available.

(2) Establish a basis against which accomplishments and resource utilization can be measured.

b. Each command, agency, and installation in the Army establishment prepares an annual COBE covering operations for which it receives funds. These COBEs are prepared in sufficient detail to identify

(1) What has to be done.

(2) When it must be done.

(3) What resources are available.

c. The COBE is prepared by each command and developed in response to program and budget guidance received from higher headquarters.

Installation Management

Section III

We have already noted that the resource management system requires installation commanders to identify the costs of their military personnel. In the future, therefore, a much higher portion of the DOD budget will be reflected annually in Army installation budgets.

2-13 Budget Formulation

At the installation level, you will be concerned with a budget cycle divided into two phases—formulation and execution.

a. The budget cycle for operation and maintenance, Army, appropriation which finances most of the day-to-day operating costs of the Army, actually starts 18 months ahead of the target budget year (BY). Most installations do not become formally involved in the actual budget until 6 to 8 months before the beginning of the target BY. As soon as the annual Army budget estimate has been finalized [following joint DOD/Office of Management and Budget (OMB) hearings on the Army budget estimate], DA revises its guidance by sending to all of its major commands revised budget and manpower guidance (BMG) in January (about 6 months before the target BY). Based on this revised guidance, each subordinate command makes necessary changes in its local plans and programs.

b. On receipt of the guidance document at the installation in October—six months prior to the BY—it is sent to the Directorate of Resource Management (DRM), who is the primary staff officer charged with financial management responsibility. After briefing the installation commander and adding the commander's desires, the DRM breaks down the guidance into terms and segments that are meaningful at the installation level. He then distributes guidance with a minimum of delay to the major activity directors (MADs).

c. The DRM develops a time-phased schedule of actions necessary for completion of the installation budget. This is similar to a suspense-date calendar.

d. Aided by his staff, the DRM establishes objectives and resource limitations, using local historical data and experience. He then prepares the draft installation BMG.

e. To facilitate and coordinate preparation of program/budgets, the staff forms a program budget advisory committee (PBAC) to serve as atop management advisory group to the commander. The Chief of Staff is normally chairman. Other members are the principal staff officers responsible for the functional areas of personnel, operations, and logistics, and other representatives as desired by the commander.

f. The committee considers all aspects of the internal management of the command.

g. Each member insures that his area of staff responsibility is accorded full consideration by the committee.

h. The use of financial data (that is, expressions of resource requirements in dollar terms) permits comparison of total input, using a common unit of measure.

i. The goals and requirements of individual areas are coordinated and molded into overall goals and requirements for the command.

j. Recommendations of the PBAC represent the consensus of the top management officials of the command.

k. The comptroller presents the draft BMG to the PBAC along with any unresolved differences that could not be settled by staff coordination.

2-14 PBAC Functions

a. Interpretation of BMG from higher authority and integration of the local commander's guidance.

b. Development of a plan for preparation of a proposed program/budget that will effectively and efficiently accomplish the command's mission.

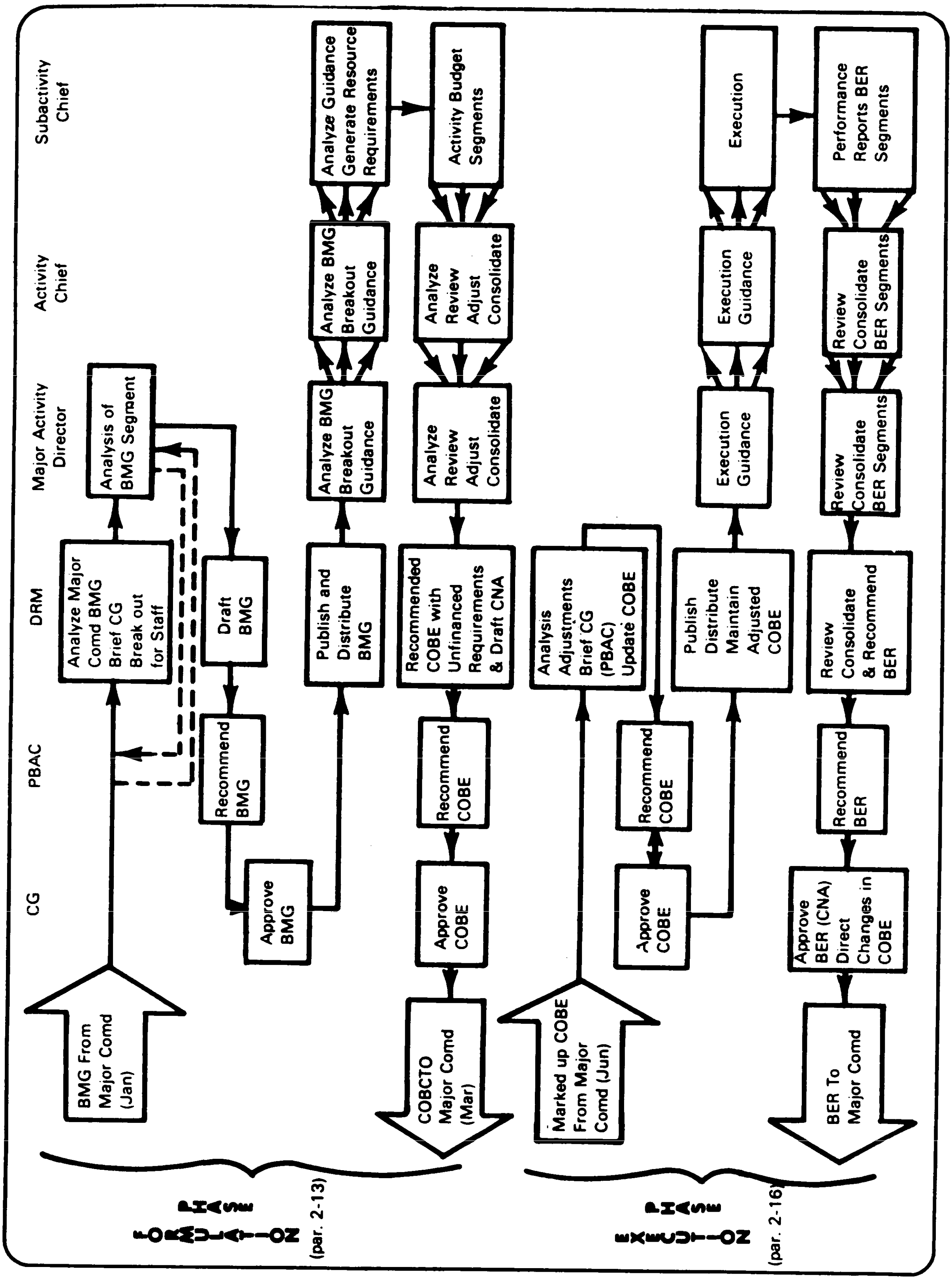


Figure 3—Installation budget cycle.

c. Application of judgment and experience to specific program areas.

d. Achievement of reasonable balance and coordination between proposed missions, activities, and resources assigned to subordinate commands and agencies.

e. Presentation of a staff-coordinated proposed command operating budget estimate (COBE) to the commander.

f. Review of the reports of program/budget execution and preparation of recommended revisions to the operating program/budget based on the results of operations.

g. Principal members of the PBAC are assisted by their subordinates who function as a junior or working PBAC. Representation in this junior group is expanded to include at least one representative of each category within each functional area. For example, the DPCA represents the provost marshal (security officer). The program/budget officer from the comptroller's office also participates as a working member. Much of the detailed work for the senior PBAC is done by the junior PBAC prior to the senior PBAC's being convened. The junior PBAC works up detailed alternative courses of action for consideration of the senior PBAC.

h. Action agencies receiving the BMG are the major activity directors (MADs). They are also frequently called program directors. Specific determinations of what is a major activity and of the designation of the MAD depend on the installation and its mission. However, primary staff officers are normally designated MADs for activities falling in their areas of primary staff responsibility. Major activities usually follow the breakdown of the Army management structure.

2-15 Major Activity Directors

For example, the director of industrial operations (DIO), is responsible for the central supply and maintenance program. Also, the Guard and Reserve forces program would belong to the director of plans and training. Physical security equipment (provost marshal's office) belongs to the director of personnel and community activities (DPCA).

a. At the installation level, organization more clearly reflects the functional management requirements, but does not clearly address the program as a whole. The installations have subdivided their programs by functional area responsibilities. The name coined for the subdivisions is "key accounts."

b. One rule that must be followed in this subdivision is that the data collected for the accounts must be identifiable to insure that when this data is combined with data concerning other key elements in the program, it does not lose its identity with the major programs that it supports.

c. Guidance is analyzed by the major activity directors and passed down to the activity chiefs who report to them. The activity chiefs analyze their guidance and pass appropriate guidance down to subactivity chiefs who report to them. For example, the DPCA is the MAD for G-641. Under him there are normally activity chiefs and subactivity chiefs (physical security managers).

d. When the guidance finally gets down to the activity/subactivity chief, it is translated into budget requirements. This is the turnaround point. Detailed budget segments are prepared by subactivity chiefs; reviewed, and consolidated by activity chiefs; again reviewed and consolidated by major activity chiefs; until the draft installation COBE is consolidated by the DRM. Requirements are justified by use of performance factors (PF) listed for budget codes in the Army management structure.

e. The basic program/budget document prepared at the installation is the activity budget schedule, reflecting, within cost guidance, dollar requirements for resources by

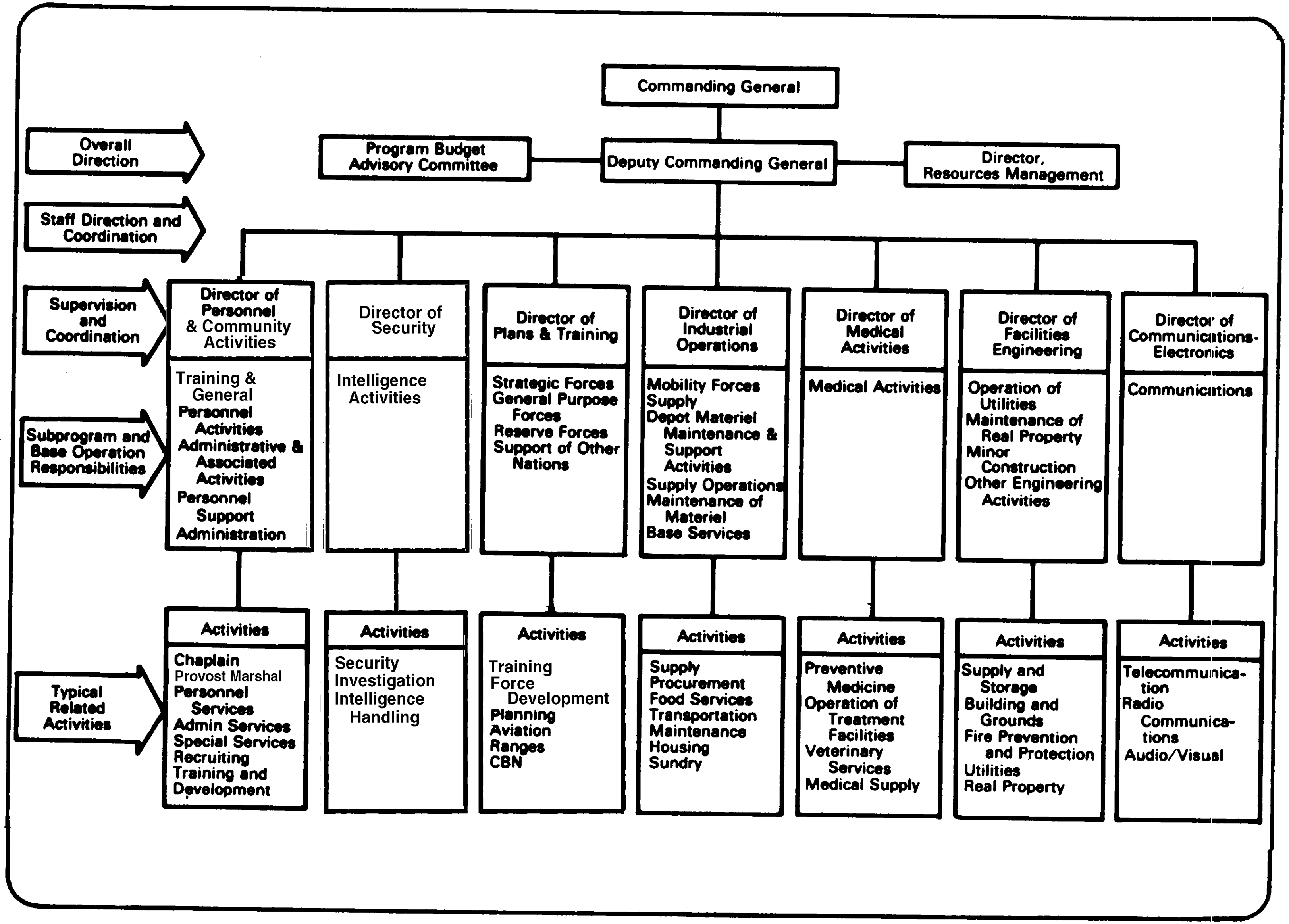


Figure 4—Typical organization for programing and budgeting (OMA).

type (element of expense), manpower by man-years and type, and work output in terms of PF. Data is projected for each quarter of the fiscal year. The same three types of data are provided for unfinanced requirements; that is, the workload considered essential for mission accomplishment and its associated resource requirements that cannot be performed within the cost guidance received. The activity budget schedule establishes a standard cost per unit of output, composed of labor, supply equipment, and other costs at the programed level of output.

f. The activity budget schedule is normally supported by schedules of temporary duty travel, supply requirements, contracts, and unfinanced requirements and a narrative statement by the activity manager. When automatic reimbursements are expected to be earned by the activity, a list of sources and anticipated amounts is also prepared.

g. Activity budget schedules are reviewed by functional category managers. Particular attention is paid to the balance of unfinanced requirements of activities having similar priorities. When balance has been achieved among activities of the same functional category, functional category managers, acting now as the working PBAC, propose adjustments in activity cost ceilings to achieve balance installation wide among all functional categories and activities.

h. The PBAC will review and make necessary modifications to the draft COBE before submitting it to the commander with its recommendations. Those items that the installation feels are necessary for the accomplishment of its mission, but cannot afford within the dollar guidance received from higher headquarters, are included in the COBE as unfinanced requirements. Unfinanced requirements are listed in order of priority with justification and impact statements supporting the installation's request for additional funds.

i. The installation COBE is a plan of action for a specific fiscal year and has a threefold purpose:

- Record activities to be conducted and resources needed for the installation's support.
- Identify action to be accomplished by each subordinate element.
- Establish basis to measure accomplishment and resource consumption.

j. Of special interest in the COBE is section I, Commander's Narrative Analysis. In this section, the commander is provided the opportunity to defend his views on the adequacy or inadequacy of his COBE which has been developed in response to guidance received from parent headquarters.

k. After review and approval, the COBE is submitted to the major command which reviews all COBEs submitted to determine consistency with guidance, magnitude, and type of resources requested and also the urgency of unfinanced requirements.

l. Major command COBEs are reviewed, adjusted, and consolidated at Headquarters, DA, and form the basis of the Army's annual apportionment request, which is submitted through DOD to OMB.

2-16 Budget Execution

a. The installation budget execution phase begins 1 October with receipt of the approved operating budget (AOB) or marked up COBE indicating the action taken in response to the DA-approved COBE. The markup of the installation COBE at this point reflects all changes to the installation's COBE resulting from budget reviews at all levels of DOD, OMB, and Congress. As such, it represents the approved installation plan of execution for the BY.

b. An approved budget establishes annual limitations and/or objectives to include the amount of expense or obligations that maybe

incurred for a specific program (or other classification) for the BY.

c. The installation marked up COBE and the AOB for the first quarter of the fiscal year are sent to the DRM for action. The DRM reviews and analyzes these documents, determines adjustments required, and informs major activity directors concerned of pertinent adjustments.

d. Through the coordinated efforts of the DRM and the working PBA, the installation program is updated. The DRM sends the original of the AOB to the finance and accounting office. Authority to obligate the Government comes to the installation in the form of a Funds Authorization Document (FAD). This authority is provided on a quarterly basis.

e. If the magnitude of changes warrants, the PBAC meets to review the revised installation program for balance in resources, levels and workloads. When satisfied with the plan of operation, the PBAC recommends that the plan be approved by the installation commander. The commander either approves the recommended program or directs that changes be made. After final approval, the program is returned to the installation DRM. The DRM finalizes, publishes, and distributes the approved installation operating program which serves as the overall plan of operations for the fiscal year.

f. The budget execution review (BER) is the midyear review report and provides the basis for funding adjustments by higher headquarters during the latter half of the current fiscal year. In preparing the BER, program and activity directors should carefully review all resource requirements to insure that estimates are accurate, and that the unfinanced requirements are completely justified to insure that no mission-essential activities are hampered by the lack of resources.

2-17 First-half-year Data

a. Actual data (experience) on expenses incurred and performance (workload) accomplished for the first 3 months (that is 1 October through 31 December).

b. Cumulative projected data for the first 6 months that include the first 3 months of actual data plus 3 months (1 October through 31 March) of projections of the expense to be incurred and the performance (workload) to be accomplished.

c. Cumulative projected data for the entire fiscal year. The last half estimated data are included in the cumulative projections or expenses to be incurred and performance to be accomplished for the entire fiscal year.

d. Segments of the BER are submitted similar to sections of the COBE; they are reviewed, analyzed, and consolidated by activity chiefs and the major activity directors, and finally, the draft installation COBE is composed of five sections.

e. Section I, Commander's Narrative Analysis, is the one in which the installation commander informs higher headquarters of major problems involved in performing assigned missions, programs, and workloads within existing resources. It is the highlight feature of the BER on which all reviews are finally focused for decision and action. It is developed under the management-by-exception concept and oriented to facilitate budget execution, management, review, and analysis processes at each succeeding level of command. See section IV, chapter 2, AR 1-1, for a more detailed explanation of the Army budgeting system.

J-SIIDS issue is based on request made to the National Inventory Control Point (NICP). Other equipment may be obtained,

153-846 0 - 94 - 2

as a result of an annual unprogrammed and unfinanced request, by providing the necessary justification for input to the command operating budget estimate (COBE).

2-18 Security Equipment Procurement Procedure

a. Security manager conducts an inspection to determine the need.

b. Determine requirement authority (DOD/DA letter, AR, directive, etc.).

c. Brief provost marshal/installation commander on installation vulnerability, equipment criticality, and need. This will also assist the commander in preparing section I of the commander's narrative analysis.

d. Coordinate with necessary installation primary staff elements and solicit documented support.

e. Prepare the installation budget forms and a security equipment decrement list to be submitted to the comptroller. (The decrement list is a priority list for items to be removed from the program if resource guidance is reduced. As such, the document list goes from lowest priority to highest priority in terms of the critical needs of the installation.)

Sample Budget Request

Section IV

Budget requests provide for police services, maintenance of order, traffic control, criminal investigations, correctional facility, and **physical security services,** equipment, and inspections. The physical security manager must review the design of Military Construction Army (MCA) projects and provide recommendations.

The cost estimate must be submitted with the appropriate transmittal document, according to local policy. DA Pamphlet 140-series explains this subject in great detail.

The samples included in the next 15 pages are physical security oriented (6 pages for COBE and 9 for SPE funding).

If the DPCA receives cuts in its request, the budget request may be returned to the installation in initial FY 80 budget guidance because of cuts in the DPCA request. If, for instance, the security manager's request for a radio network was not funded, he must submit a second request for special equipment finding to the installation DRM.

Sample Estimates
And request for SPE Funding
(next 15 pages)

FY 80 COMMAND OPERATING BUDGET ESTIMATE
SCHEDULE OF EQUIPMENT

ITEM DESCRIPTION	PURPOSE/USE	QTY	UNIT COST	TOTAL COST	AMS BUDGET ACCOUNT CODE	PRIORITY CATEGORY
VH Vehicle Radio	To provide communications for 4 newly authorized MP sedans, 1 per quarter.	4	$1,200	$4,800	.G6000	
Desk, double pedestal	Replace unserviceable item at post confinement facility, 1 per quarter.	4	315	1,260	.G6000	
Anti-intrusion device	To protect sensitive areas in: Defense Service Center, 1st Qtr. CDC Agency, 1st Qtr.	10	400	4,000	.G6000	
Vehicle speed radar	Improve traffic control in the 1st and 3d Qtrs.	2	3,000	6,000	.G6000	
Camera, 4x4	For investigative purposes, 1st Qtr.	1	800	800	.G6000	
Nontactical radio network	Improve police and security communications				.G6000(2300)	
Repeater		1	2,700	2,700	.G6000	
Consolette		2	1,750	3,500	.G6000	
Base Station		1	3,300	3,300	.G6000	
2-channel mobile radios		7	1,315	9,205	.G6000	
Hand-held portables		17	1,117	18,989	.G6000	
Antennas		4	1,750	7,000	.G6000	
			TOTAL	$62,554		

Sample COBE (1 of 6 pages).

FY 80 COMMAND OPERATING BUDGET ESTIMATE

SECTION I - REQUIREMENTS   ACTIVITY TITLE: Provost Marshal (Security)

ELEMENT OF EXPENSE	PERIOD	PERIOD	PERIOD	PERIOD	FY TOTAL
1000 PERSONNEL SERVICES & EXPENSES	$	$	$	$	$ 18,050
1110 Personnel Compensation GS	( )	( )	( )	( )	(16,000)
1120 Personnel Compensation WB	( )	( )	( )	( )	( )
1210 Personnel Benefits GS	( )	( )	( )	( )	(2,050)
1220 Personnel Benefits WB	( )	( )	( )	( )	( )
2100 TRAVEL & TRANSPORTATION					35,700
2200 TRANSPORTATION OF THINGS					
2300 RENTS COMMO, UTILITIES					
2310 Rents	( )	( )	( )	( )	( )
2320 Communications	( )	( )	( )	( )	( )
2330 Purchased Utilities	( )	( )	( )	( )	( )
2500 OTHER CONTRACTUAL SERVICES					37,290
2511 Purchased Equip Maintenance	( )	( )	( )	( )	( )
2572 Other Purchased Services	( )	( )	( )	( )	( )
2600 SUPPLIES & MATERIALS					145,700
2610 Supplies Except POL/ADP/MED	( )	( )	( )	( )	( )
2620 Acft POL	( )	( )	( )	( )	( )
2640 Other POL	( )	( )	( )	( )	( )
2650 ADP Supplies	( )	( )	( )	( )	( )
2660 Medical Supplies	( )	( )	( )	( )	( )
2670 Aviation Supplies	( )	( )	( )	( )	( )
2700 SERVICE CHARGE FUNCTION					
2770 Rel Prop & Util Rent Equip	( )	( )	( )	( )	( )
3100 EQUIPMENT					16,860
3100 Capital Equip-Except MED/ADP	( )	( )	( )	( )	(16,860)
3140 Capital Equip-Medical	( )	( )	( )	( )	( )
9900 ALL OTHER NOT SHOWN					
TOTAL REQUIREMENTS	$	$	$	$	$ 253,500

SECTION II - WORKLOAD

COBE summary (2 of 6 pages).

ALM-61-3550-H5
61-500

SECTION III - MANPOWER

GS AUTHORIZED 2 | WB AUTHORIZED 0 | TEMP HIRE AUTHORIZED 0
GS ACTUAL 2 | WB ACTUAL 0 | TEMP HIRE ACTUAL 0

SECTION IV - FINANCING

DIRECT FUNDS 71,400 OMAR $	REIMBURSEMENTS FUNDED $ 0		REIMBURSEMENTS AUTOMATIC $ 12,500	TOTAL FUNDS $253,500	
ELEMENTS OF EXPENSE	PERIOD	PERIOD	PERIOD	PERIOD	FY TOTAL
1000 FY REQUIREMENTS FY FINANCED					
2100 FY REQUIREMENTS FY FINANCED					
2200 FY REQUIREMENTS FY FINANCED					
2300 FY REQUIREMENTS FY FINANCED					
2500 FY REQUIREMENTS FY FINANCED					
2600 FY REQUIREMENTS FY FINANCED					
2700 FY REQUIREMENTS FY FINANCED					
3100 FY REQUIREMENTS FY FINANCED					
9900 FY REQUIREMENTS FY FINANCED					
FY TOTALS 1. REQUIREMENTS 2. FINANCED 3. UNFINANCED					

COBE summary continued (3 of 6 pages).

FY 80 COMMAND OPERATING BUDGET ESTIMATE

TRAVEL & TRANS OF PERSONS

DESCRIPTION/PURPOSE	DATES	NUMBER PER TRIP	COST	AMS BUDGET ACCOUNT CODE	PRIORITY CATEGORY
Trips by PM personnel to conduct liaison at TRADOC headquarters, estimated	As necessary	NA	$ 2,000	.G6000	
One trip per quarter for PM to conduct liaison at headquarters TRADOC, estimated $25 per trip	1 day Qtr	2	200	.G6000	
Prisoner escort. Pick up deserter from civilian law enforcement agencies and/or FBI offices. Historical estimates, 100 trips at $200 per trip	NA	1	20,000	.G6000	
Security investigations, estimated					
Physical security 30 at $100 each	NA	1	3,000	.G6000	
Security clearance 70 at $100 each	NA	1	7,000	.G6000	
Off-post physical security inspections. 175 inspections at $20 each	NA		3,500	.G6000	
		TOTAL	$35,700		

Sample COBE continued (4 of 6 pages)—Travel and transportation.

FY 80 COMMAND OPERATING BUDGET ESTIMATE

CONTRACTUAL SERVICES

PERIOD OF THE CONTRACT	PURPOSE OF CONTRACT	AMS BUDGET ACCOUNT CODE	AMOUNT	PRIORITY CATEGORY
1 Jul-30 Jun	Security guards 8 each for Camp Aims. Provide security for PX, commissary, and finance office. Annual contract. Awarded based on AR 235-5. Evaluation of Commercial-Industrial Activities (CITA).	.G6000	$28,400	
1 Jul-30 Jun	Security gate guard 1 each during daytime for Defense Service Center.	.G6000	2,522	
1 Jul-30 Jun	Intrusion detection device contract:			
	Small arms repair shop		348	
	Main post commissary		432	
	Main post finance		744	
	Branch finance		540	
	Bright Hall		520	
	Swynett complex		530	
	FAOOM		559	
	FANOOM		431	
1 Jul-30 Jun	Link teletype (Law Enforcement Network, VA)		2.474	
		TOTAL	$37,500	

Sample COBE continued (5 of 6 pages)—Contractual services.

FY 80 COMMAND OPERATING BUDGET ESTIMATES

SUPPLIES AND MATERIALS

DESCRIPTION AND PURPOSE	AMS BUDGET ACCOUNT CODE	QTY	UNIT COST	TOTAL COST	PRIORITY CATEGORY
Estimated health and comfort items for prisoners in post confinement facility	.G6000	NA	NA	$ 32,400	
Self-service supply center administrative supplies (based on historical usage)	.G6000	NA	NA	8,000	
Traffic control materials	.G6000	NA	NA	31,300	
POL for military police vehicles based on 400,000 miles per year at $.04 per mile	.G6000	NA	NA	16,000	
Repair parts for small arms, communications equipment, etc.	.G6000	NA	NA	20,000	
Decals for vehicles	.G6000	NA	NA	38,000	
			TOTAL	$145,700	

Sample COBE continued (6 of 6 pages)—Supplies and materials.

10 November 1979

SUBJECT: Request for Special Equipment (SPE) Funding

Commander
US Army Military Police School/
Training Center and Fort McClellan
ATTN: ATZN-DRM
Fort McClellan, Alabama 36205

1. Request SPE funding in the amount of $45,000 be made available for the purchase and installation of equipment required to renovate and expand the nontactical radio network of the security police force.

2. The timing of this funding request has been accelerated by the change in mission storage and shipment requirements and approved expansion of personnel and other equipment to the security force TDA. When the security mission increased in criticality, number of items, and shipment procedures, the current communication network became overextended, outdated, and lacked the number required to provide for a safe and secure environment during operations.

3. The present nontactical network is restricted in its range and cannot make contact with security patrols during convoy operations while off the installation. Additionally, the current network will not provide adequate communication for the installation during periods of war emergency, installation confrontations, terrorists activities, natural disasters, or other situations which may result in the disruption of normal communications.

4. Following is a listing of the required items with acquisition costs.

Item	Quantity	Cost
Repeater	1	$ 2,700
Consolette	2	3,500
Base station	1	3,300
2-channel mobile radios	7	9,205
Hand-held portables	17	18,989
Antennas	4	7,000
Total		$44,694

Sample SPE funding request (1 of 9 pages).

5. An economic analysis for this requested action was done by the operational research/systems analysis branch. The purchase alternative is recommended based on the analysis and a copy of each, purchase v. lease, is inclosed.

4 Incl
as

GARY R. MOORE
CPT, MPC
Security Manager

Coordination:

PM: Concur/Nonconcur________Date__________

DPTSEC: Concur/Nonconcur________Date__________

Sample SPE funding request continued (2 of 9 pages).

SUMMARY OF PROJECT COSTS

1. Submitting Component: Security Branch, Provost Marshal Office

2. Date of Submission: 10 November 1979

3. Project Title: Funding Request for Nontactical Radio Network

4. Description of Project Objective: Update Overaged Current System

5. Alternative: Purchase 6. Economic Life: 5 years

7.			8. Project Costs		
	a. Nonrecurring	b. Recurring	c.	d.	e.
Project Year	Investment	Operations	Annual Cost	Discount Factor	Discounted Annual Cost
1	46,521.10	272.74	46,793.84	.954	44,641.32
2		272.74	272.74	.867	236.47
3		272.74	272.74	.788	214.92
4		272.74	272.74	.717	195.55
5		272.74	272.74	.652	177.83

9. TOTAL 45,466.09

10a. Total Project Cost (discounted) 45,366.09

10b. Uniform Annual Cost (without terminal value) 9,093.22

11. Less Terminal Value (discounted) -0-

12a. Net Total Project Cost (discounted) 45,366.09

12b. Uniform Annual Cost (with terminal value) 9,093.22

13. Source Derivation of Cost Estimates (use as much space as required): See attached documentation.

a. Nonrecurring Costs: (Entries may vary.)
   1) Research & Development
   2) Investment:

b. Recurring Cost: (Entries may vary.)

c. Net Terminal Value: Not available.

d. Other Considerations: (Entries may vary.)

Sample SPE request continued (3 of 9 pages)—Enclosure 7.

SUMMARY OF PROJECT COSTS

1. Submitting Component: Security Branch, Provost Marshal Office

2. Date of Submission: 10 November 1978

3. Project Title: Funding Request for Nontactical Radio Network

4. Description of Project Objective: Update Overaged Current System

5. Alternative: Lease

6. Economic Life: 5 years

7.

8. Project Costs

Project	a. Nonrecurring Investment	b. Recurring Operations	c. Annual Cost	d. Discount Factor	e. Discounted Annual Cost
1	4,683.25	14,613.46	19,296.71	.954	18,409.06
2		14,613.46	14,613.46	.867	12,699.87
3		14,613.46	14,613.46	.788	11,515.41
4		14,613.46	14,613.46	.717	10,477.85
5		14,613.46	14,613.46	.652	9,527.98
9. TOTAL					62,630.17

10a.	Total Project Cost (discounted)	62,630.17	
10b.	Uniform Annual Cost (without terminal value)		12,526.03
11.	Less Terminal Value (discounted)		-0-
12a.	Net Total Project Cost (discounted)	62,630.17	
12b.	Uniform Annual Cost (with terminal value)		12,526.03

13. Source Derivation of Cost Estimates (use as much space as required) See attached documentation.

a. Nonrecurring Costs: (Entries may vary.)
   1) Research & Development
   2) Investment:

b. Recurring Cost: (Entries may vary.)

c. Net Terminal Value: Not available.

d. Other Considerations: (Entries may vary.)

Sample SPE request (4 of 9 pages)—Enclosure 2.

OTHER FACTORS FOR CONSIDERATION (PURCHASE vs. LEASE)

1. Status Quo:
Based on information received from various security supervisors and patrolmen, the current radio network is overaged and maintenance costs are high. Additionally, the security branch received an IG deficiency because we could not reach all security patrols.

By installing a new system, all of the above problems could be alleviated.

2. Purchase:
a. Benefits:
(1) The provost marshal would own the equipment. We could modify it to suit our needs.
(2) A one-time cost would be incurred which eliminates much bookkeeping.

b. Costs:
(1) Return on investment for state-of-the-art updates would be less than with a lease agreement.
(2) Maintenance and installation costs are the same as leasing.

3. Lease:
a. Benefits:
(1) The return on investment for leased items is higher than for purchased equipment. For state-of-the-art updates, commercial firms will allow credit for investment-to-date.
(2) The total cost of the radio network can be spread out for 5 years, at which time we would own the equipment.

b. Costs:
(1) As shown in the Present Value equation, the total cost would be $17,119.73 higher for lease.
(2) Associated with the lease is an increased nonquantifiable bookkeeping cost (monthly entries for 5 years).
(3) To modify a leased radio system, we have to get the leasor's permission and pay them for the modification.

4. Extent of the System:
Some further review of the number of MX Portables and Pagecom Pagers needed should be made to insure that all units listed are necessary.

5. Contact with Other Suppliers:

Sample SPE request (5 of 9 pages)–Enclosure 3.

6. Use of Army Tactical Radios:
This alternative was found unsuitable for the following reasons:
a. Wide band radios, as tactical radios, are restricted to tactical use only.
b. The frequencies assigned to the security branch are outside the tactical radios' capabilities; they are FM radios and our frequencies are VHF.
c. Tactical radios are much more expensive than nontactical ones, and this use would not be cost effective to the US Army as a whole.

Sample SPE request (6 of 9 pages)—Enclosure 3 continued.

PRESENT VALUE EQUATIONS FOR LEASE AND PURCHASE OF NONTACTICAL RADIO EQUIPMENT

PURCHASE

PV_p = 41837.85 (PV_1) + 3732.85 (PV_1) + 950.40 (PV_1) + 272.74 (SPV_5)
= 41837.85 (.954) + 3732.85 (.954) + 950.40 (.954) + 272.74 (3.977)
= 39913.31 + 3561.14 + 906.68 + 1084.69
= 45465.82

Explanation of Costs:
41837.85 = Cost of equipment purchase
3732.85 = Antenna installation
950.40 = Equipment installation
272.74 = Annual maintenance cost

LEASE

PV = 3732.85 (PV_1) = 950.40 (PV_1) = 14613.46 (SPV_5)
= 3732.85 (.954) + 950.40 (.954) + 14613.46 (3.977)
= 3561.14 + 906.68 + 58117.73
= 62585.55

Explanation of Costs:
3732.85 = Antenna installation
950.40 = Equipment installation
14613.46 = Annual cost (lease + maintenance)

LEASE COST ALTERNATIVE:

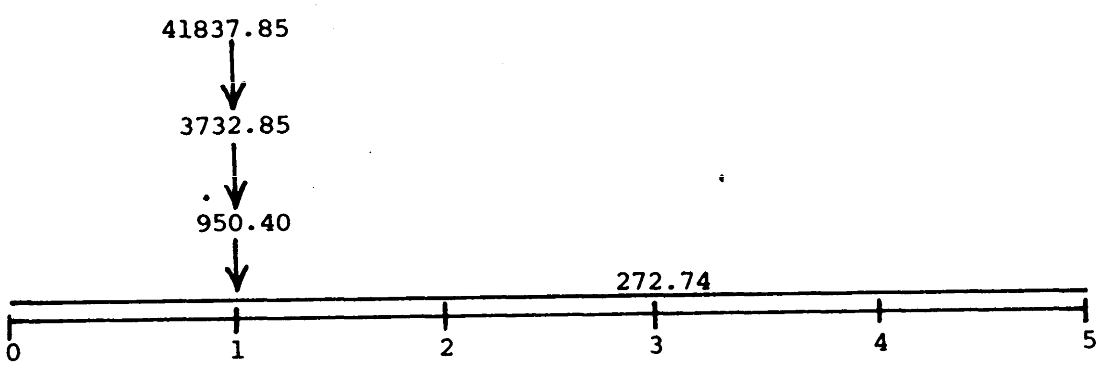
Purchase of equipment

Sample SPE request (7 of 9 pages)—Enclosure 4.

TIME LINE FOR INVESTMENT

ECONOMIC LIFE   5 Years

PURCHASE OF NONTACTICAL RADIO NET EQUIPMENT



EXPLANATION OF COSTS

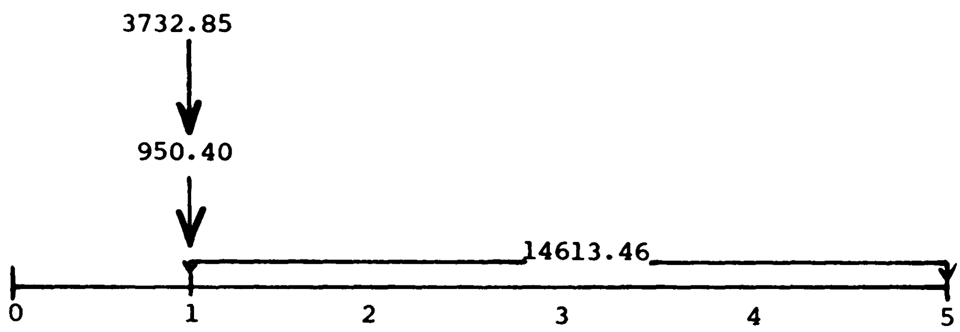
41837.85 - Purchase of Radio Equipment
3732.85 - Antenna Installation
950.40 - Equipment Installation
272.74 - Annual Maintenance

Sample SPE request (8 of 9 pages)—Enclosure 4 continued.

TIME LINE INVESTMENT

ECONOMIC LIFE 5 Years

LEASE OF NONTACTICAL RADIO NET EQUIPMENT



EXPLANATION OF COSTS

14613.46 - Annual Lease Cost and Maintenance
 14340.72 - Annual Lease Cost
 272.74 - Annual Maintenance
3732.85 - Antenna Installation
950.40 - Equipment Installation

Sample SPE request (9 of 9 pages)—Enclosure 4 continued.

Review and revision of tables of organization and equipment (TOEs) is accomplished on a recurring basis, coinciding with HQDA planning requirements and the Army implementation of the Five-Year Defense Program (FYDP) as discussed earlier.

The TOE Documentation Program is controlled by the TOE program letter and schedule. This letter specifies the TOE to be developed or revised during the fiscal year, and is published in July and updated in January. Security managers are not involved in the revision and development of TOEs. This action depends on the TOE proponent agency within the TRADOC school system. It is based upon and in concert with, DA approved doctrine and concepts, etc. (See AR 310-31.)

2-19 Security Manager's Interface

a. Security managers, at various times, must be involved with revision of modification tables of organization and equipment (MTOEs) and tables of distribution and allowances (TDAs)-mainly the latter. This involvement usually requires an interface with the supporting force development officer or the next higher headquarters operation section (S3) to prepare documents in accordance with the Army Authorization Documents System (TAADS) which is a system used for:

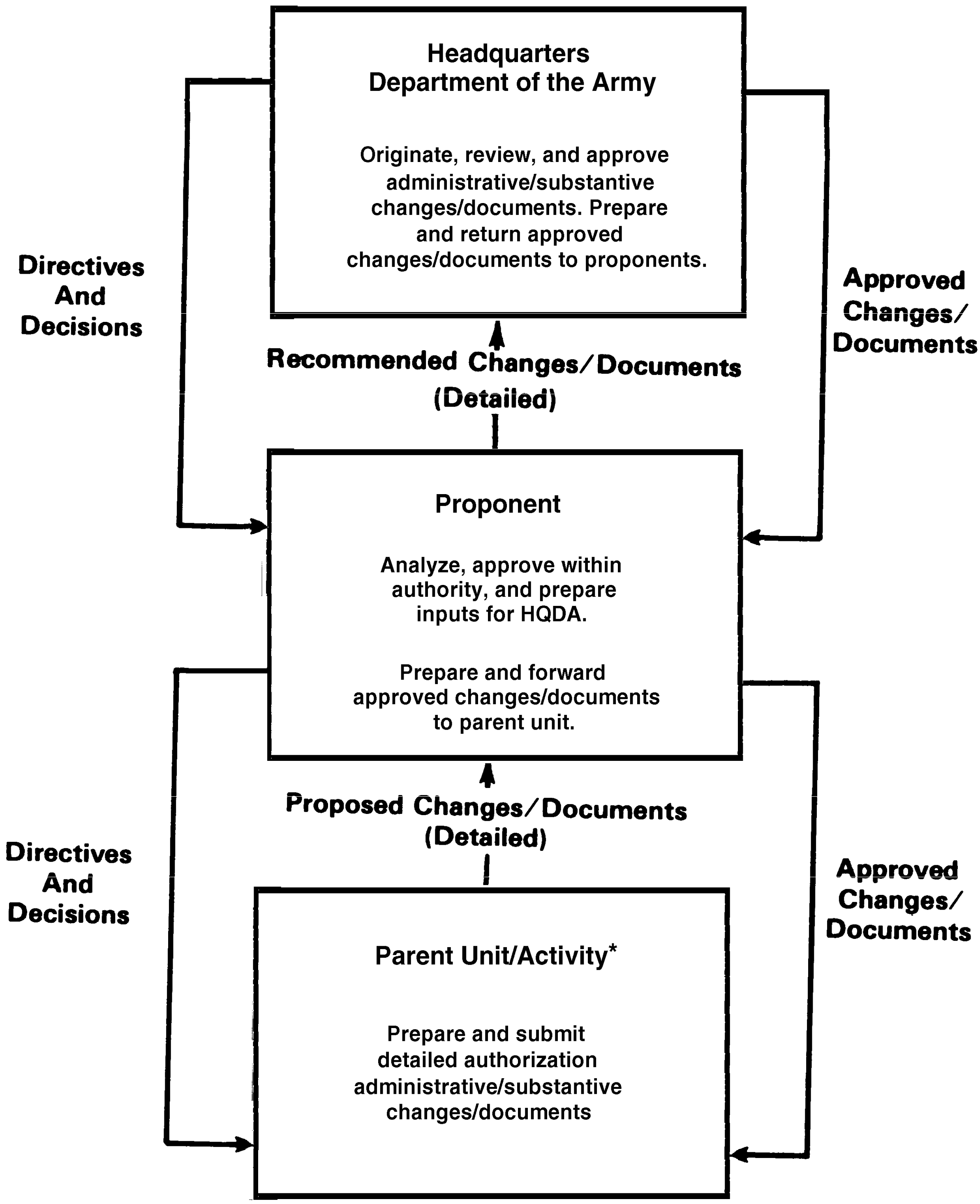
- ❑ Developing organizational structures
- ❑ Requirements
- ❑ Personnel authorizations and equipment.

b. The final product of this system is a unit's authorization documents (MTOE/TDA), which provide for subsequent personnel and equipment transactions. The MTOE provides the commander with the means to modify or adjust the DA approved TOE to meet specific operational requirements. The TDA, on the other hand, establishes its own organizational structure to meet the needs of each specified unit. A flow chart showing the processing of a TAADS authorization document is at figure 5. Authorizations to support this document are as follows:

- MTOE
- TDA
- Augmentation TDA
- Mobilization TDA.

c. TDA security units organized to support the Army's peacetime posture may not be sufficient in terms of personnel strength and equipment. The requirements column of the TDA must be based on requirements recognized in an approved manpower survey. Adjustments by the survey authority maybe made when changes in mission, function, or workload occur between manpower surveys. Requirements for a new TDA unit must be based on the mission, projected workload, and applicable staffing guides.

d. The manpower authorizations column of the TDA must be based on allocations of resources, and normally will be equal to or less than the manpower reflected in the requirements column. When authorizations are less than requirements, reduced capabilities must be reflected in the appropriate paragraphs of section I of the TDA.



* Security manager involvement

Figure 5—Flow chart for TAADS data.

e. Grades of DA civilian personnel positions in the TDA must be established by application of civil service and DA civilian personnel policies, regulations, and procedures.

f. Organizational structures of TDA units must adhere to applicable DA regulations governing organization of specific units; or in the absence of such regulations, they must adhere as closely to the appropriate DA staffing guide as local conditions permit.

g. Military and civilian manpower utilization policies in AR 570-4 must be followed when organizing and staffing TDA units to perform security missions.

2-20 Manpower Management

The objective is to achieve optimum use of manpower in accomplishing the security mission.

a. The security manager must realize that the two primary constraints on manpower are:

(1) Man-years generated during a fiscal year.

(2) Strength at the end of a fiscal year.

b. The total strength of an activity at any given time in the year is important because it is the basis for computing man-years.

c. As security strengths change during a fiscal year, adjustments must be made to:

(1) Total man-years and, if appropriate,

(2) End-year strengths.

Manpower planning and allocation documents, as discussed previously, are as announced in Chapter IV of the Program and Budget Guidance (PBG) provided to major activity directors (MADs).

2-21 Establishing Manpower Requirements

a. The security manager must obtain the following documents to prepare his requirement:

(1) TOE manpower authorization criteria

(2) DA staffing criteria

(3) DA staffing guides

(4) Manpower surveys

(5) Various work measurements

(6) The physical security plan.

b. The civilian personnel officer will actively participate in TDA development involving civilian security positions. Civilian position structures in the TDA will be in accordance with regulations of:

(1) The office of management and budget

(2) Civil Service Commission (CSC)

(3) HQDA.

2-22 Grade and Position Change

a. To change security grade level or position at the local level, unless instructed otherwise, must be done IAW the following:

(1) Civilian Personnel Regulation 501.

(2) Job reengineering.

(3) Civil Service Commission Research & Development Engineering Grade Evaluation Guide.

(4) Civil service classification guidance.

b. Grade levels and position structure of positions in grade GS-15 and below, and in wage board pay categories may be submitted

as proponent-approved, unless HQDA instructs otherwise.

c. Evaluation of civilian personnel officer positions are subject to the provisions of Civilian Personnel Regulation (CPR) 501.

d. Application of job evaluation decisions of the CS or HQDA is mandatory. Action on such mandatory decisions must be taken in accordance with civilian personnel regulations and instructions, even though application results in grade levels that exceed the current approved TDA.

e. Prior approval requirements. The security manager must realize that successive echelons of command are not authorized to establish prior approval requirements beyond the provisions of CPR 501, unless determined to be necessary to improve position management and the civilian position structure. The HQDA policy of decentralizing authority for civilian personnel management and for position classification to the lowest practicable level must. be observed both in principle and in practice.

f. Civilian grades listed in DA-approved TDA. Civilian grades listed in DA-approved TDAs are not authorized until finalized by the security element's supporting civilian personnel office in accordance with the above paragraphs. DA review normally will be accomplished on a post audit basis. Comments addressing civilian positions in approved TDAs, if any, will be furnished separately by DAPE-CPP.

2-23 Proponent-Initiated Changes

a. The organization structure of security units and activities may be changed at the initiative of commanders. Changes may be necessary to respond to changes in mission or to realine resources and organizational elements for greater security mission efficiency.

b. Proponent-initiated changes must comply with organizational policies, as set forth in chapter 2, AR 310-49.

c. Changes in the organization and manning of units and activities must conform to the manpower management policies in AR 310-49, and to information on position categories, classifications, and grading.

d. Requests for additional security personnel spaces required because of increased workload or similar factors must be made in accordance with AR 570-4.

2-24 Justification For Personnel Changes

a. Justification is an explanation of the situation and circumstances which require personnel changes to cope with the security mission.

(1) Your justification is the major basis on which the Army staff forms its judgment regarding the request.

(2) Explanations must be sufficiently clear, well-organized, concise, and complete to allow an analyst who is unfamiliar with the unit and local conditions to understand the rationale for the proposed action.

b. Organization charts and diagrams help to clarify the reasons for a justification proposal.

c. A citation of Army directives, previously obtained approval of actions, and approved manpower survey reports frequently are adequate justification.

d. Section VI shows conditions that influence personnel spaces and the actions re-

quired by proponents to justify specific changes.

e. When new security organizational elements are formed, an explanation of the mission or functions of the newly formed organization and an estimated workload will often suffice to justify positions, grades, and MOSs of members.

(1) Job descriptions provided must be fully explained to assist in the justification.

(2) To further substantiate the requirement for a position, the grade and MOS or civilian series code, workload data, and an indication why the work is performed, must be included in the justification.

f. Guidance for preparation and sub mission of justification for security personnel changes in TAADS is reflected in AR 310-49.

2-25 Justification for Security Personnel and Equipment

a. The security manager must document necessary justification in accordance with:

(1) AR 570-2

(2) AR 611-1

(3) AR 611-101

(4) AR 310-34

(5) AR 310-49

(6) AR 750-43.

b. As a security manager, you realize that TDA units rely primarily on manpower to establish manpower requirements. Therefore, between surveys, manpower survey forms must be used and documented to assist in developing changes in requirements caused by changes in the activity's security mission and/or workloads.

c. To increase the personnel strength level of the local security office in an effort to supplement the TDA, you will be required to justify the increase IAW DA Pamphlet 570-4, The Manpower Procedures Handbook. Acting as a check and balance to strength levels, manpower surveys by specialized teams are conducted on a programed basis; therefore, as a security representative of the commander, the burden of proof that additional manpower is needed to accomplish the security mission rests with assessment of individual capabilities and documentation of normal workloads.

d. In accomplishing this documentation, there are several survey documents that present data about the operation of the security office in terms of:

(1) Organization

(2) Manpower utilization

(3) Workloads

(4) Estimated manpower requirements in relation to existing guides.

e. The security manager, when preparing for manpower surveys, must take a two-prong approach—(1) strong justification must be documented to prevent loss of existing manpower, and (2) strong detailed justification must be documented to obtain additional manpower spaces. Survey documentation involves the following forms:

(1) DA Form 140-1 (Remarks)

(2) DA Form 140-2 (Schedule A - Manpower Inventory)

(3) DA Form 140-3 (Schedule T-Identification of Manpower)

(4) DA Form 140-4 (Schedule X - Manpower and Workload Data)

(5) DA Form 140-5 (Schedule A - Manpower Inventory Continuation Sheet).

f. Initial entries on the forms must be made by the security manager, and the applicable portions must be completed during the on-site visit by the manpower teams.

2-26 Staffing Guides

Appropriate staffing guides must be used in preparing TDAs. It is essential that the security manager use the correct yardstick for manpower appraisals and requirements to accomplish the following:

(1) Indicate the total number of positions required to perform a security function.

(2) Consider:

(a) Annual leave
(b) Sick leave
(c) Training
(d) Orientation
(e) Other activities not contributing directly to the performance of the designated function.

2-27 Yardstick Examples

a. The following yardstick determination for 8-hour-day/7- and 5-day-week positions involve basic man-years (BMY) and nonavailable time (NAT) computations for security positions. The computations are a modified version of those outlined in DA PAM 570-4; however, they have been accepted by various manpower survey teams as unique to a security unit or depot.

b. Eight-Hour-Day-Week Position

(1) Determine nonavailable time (NAT):

(a) Days off (2 days per week)=2 x 8 x 52 = 832 hours.
(b) Leave (30 days per year)=30 x 8 = 240 hours.
(c) Sick (1/3 day per month) = 1/3 x 8 x 12 = 32 hours.
(This should be based on historical records taken from sick slips but in lieu of accurate data, 1/3 day per month is acceptable average per man.)
(d) Training (3 days per month) = 3 x 8 x 12 = 288 hours.
(Again, this number must be based on actual and programed training, including time for SQTs, SQT preparation, actual job training, and mandatory unit training such as RR/EO, etc., per man.)
(e) Total nonavailable time = 1,392 hours.

(2) Determine available time (AT):

AT= BMY - NAT 2,920 - 1,392 = 1,538

(3) Determine yardstick (YS):

YS = BMY divided by AT
2,920 divided by 1,528 = 1.9 men per required position.

(a) For a 24-hour-7-day-week position, multiply the basic yardstick by 3 (5.7).
(b) For a 16-hour-day-7-day-week position, multiply the basic yardstick by 2 (3.8).
(c) For less than a 7-day position, multiply the proper yardstick by the number of days required and divided by 7 (such as, 24-hour day, 6 days per week = $\frac{1.9 \times 3 \times 6}{7}$ = 4.9).

c. Eight-Hour-Day-5-Day-Week Position

(1) It is necessary to determine basic man-years.

(2) Determine nonavailable time without considering days off, since it is a 5-day week position:

(a) Leave (30 days per year) = 30 x 8 = 240 hours.
(b) Sick (1/3 day per month) = 1/3 x 8 x 12 = 32 hours (determined the same as for 7-day week position).
(c) Training (3 days per month)= 3 x 8 x 12 = 288 hours (determined the same as for 7-day week position).
(d) Total nonavailable time= 560.

(3) Determine available time:

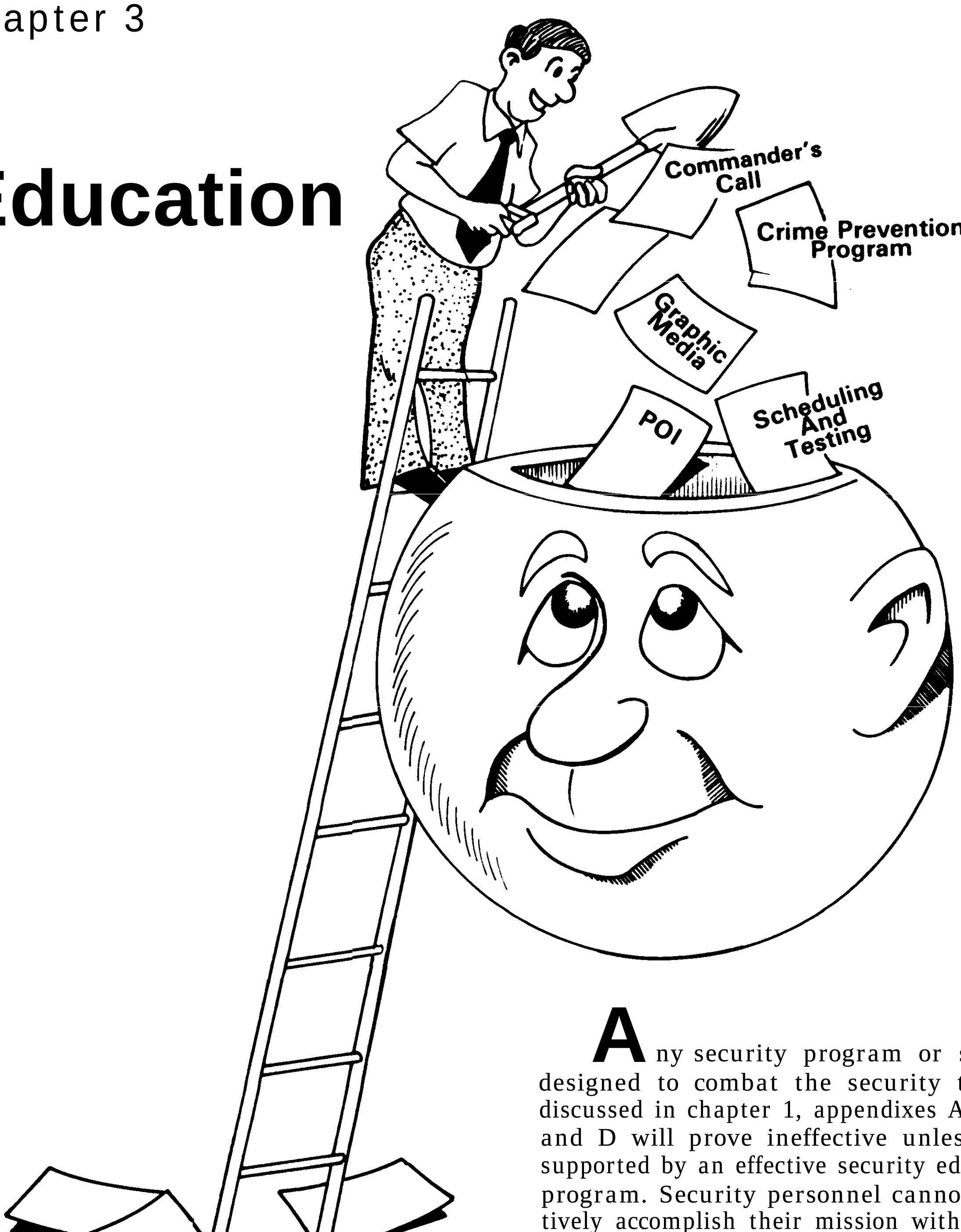
2,920-560 = 2,360

(4) Determine yardstick:

2,920 divided by 2,360= 12.

Chapter 3

Education



Any security program or system designed to combat the security threats discussed in chapter 1, appendixes A, B, C, and D will prove ineffective unless it is supported by an effective security education program. Security personnel cannot effectively accomplish their mission without the active interest and support of everyone on the installation. Such interest and support can be secured only through an effective security education program.

3-1 Program Considerations

a. It is obvious from a review of the security threats as presented, that a security education program must approach security from a total package, comprehensive-360-degree viewpoint. It must be concerned not only with physical security measures designed to prevent such purely criminal acts as pilferage; but just as important, with counterintelligence measures designed to provide security of classified intelligence information and materials. The close relationship of the two types of security is made evident from a review of the Counterintelligence Survey Checklist in FM 30-17, Counterintelligence Operations. The relationship and importance of physical security to all other security is also well documented in DA Pam 380-1. Both of these documents are highly recommended reading for the physical security manager.

b. It is also essential that the security education program include all pertinent aspects of the crime prevention program (ARs 190-31, 190-33, 195-10, and FM 19-20). Many aspects of this program have a direct personal application to all installation personnel.

c. The individual and collective concern of every soldier and Department of the Army (DA) civilian is involved in protection efforts. Security education must be designed to supplement mission accomplishment and be considered essential to the successful implementation of a physical security program.

d. Your educational program should encourage prompt reporting of security breaches and attempt to:

- Reduce security infractions and violations.
- Act as a communications feedback for improved protective measures.
- Reduce vulnerabilities.
- Instill security consciousness, which will solicit potential-threat information.

e. The essential interrelationship of both types of security, plus the need for close coordination between Military Police and Army Counterintelligence personnel in the formulation and operation of a security education program were considered in preparing this chapter.

3-2 Program Formulation

To insure integration of security education, your plan must be developed at the installation level, which will require actions by the major commands. Based upon vulnerability and criticality, statistical data of incidents and criminal information formulation must complement both crime prevention and military intelligence educational efforts.

3-3 Program Objectives

a. The objectives of a security education program are to acquaint all personnel with the reasons for security measures and to insure their cooperation. The assumption by installation personnel (military and civilian) that they are not concerned with security unless they work with classified matter or in a restricted area must be overcome. It must be impressed upon them and be continually reiterated that a locked gate or file cabinet does not constitute an end in itself, but is merely an element in the overall security plan.

b. A continuous program should be presented to selected audiences (primarily supervisors and other key personnel) on timely and applicable topics to develop and foster a high degree of security consciousness.

3-4 Educational Requirements

Security consciousness is not an inherent state of mind—it must be acquired. Many people are naive and trusting, and are

153-846 O - 94 - 3

inclined to accept things at face value, Desirable as these characteristics are, they are not conducive to vigilance or security consciousness. Structural and mechanical aids to security are valueless without the active support of all personnel. All installation personnel must be made aware of the constant threat of breaches of security and of their individual responsibilities to detect and thwart such threats. A continuous and forceful education program provides the constant awareness that successful security demands.

3-5 Personal Presentations

Very effective at commander's call.
Requires formal instruction at the unit and activity level.
Technical advice may be presented by the provost marshal or security manager.
Security content is presented in accordance with the 190-series Army regulations.

3-6 Graphic Media Aids

Posters –are effective since they may be large in size, brief and to the point, and impact their message at a glance. Posters should be displayed in locations where the majority of people pass and/or congregate.

Placards –used where attention is necessary and people are expected to loiter and have time to read, such as bulletin boards, telephone booths, vending machines and recreation areas.

Leaflets –are economical and are usually pocket size for easy carrying. Distribution of leaflets is determined by the commander or activity chief.

3-7 Indoctrination

AR 380-5 requires the commander to establish security indoctrination and education programs within his command and insure the following:

a. Each individual is indoctrinated and kept proficient in the particular security procedures which apply to him in the performance of his duties.

b. All personnel are aware of their security responsibilities.

c. All newly assigned personnel must be given security indoctrinations. The reading of printed security regulations is not sufficient to insure complete understanding. Indoctrination should consist of a general orientation on the need for and dangers to security, and the individual's responsibility in preventing infractions. It should include a discussion of those hazards common to all personnel, with emphasis on the dangers of loose talk and operational carelessness. It should define general security measures in effect, such as the pass system, private vehicle control, and package inspection. The security indoctrination is an introduction to the subject as applied to the particular installation. Further instruction should be applicable to the individual's duty assignment.

d. Further orientation, on an initial and annual basis, is prescribed by AR 381-12, Subversion and Espionage Directed Against the US Army and Deliberate Security Violations.

e. AR 360-81, The Command Information Program, discusses news media that can be used in security education programs, including those prescribed by AR 381-12.

3-8 Crime Prevention

All security education programs should include materials on the crime prevention programs (AR 190-31, AR 195-10, FM 19-10, and FM 19-20) which are designed to reduce crime. This is done by eliminating or

neutralizing factors that cause individuals to commit criminal acts and that remove or minimize opportunities for committing such acts.

FM 19-20 provides detailed guidance on conducting a crime prevention program. Such a program includes both the conduct of crime prevention surveys for the purposes mentioned in above paragraph, and an education program to emphasize security consciousness on the part of all personnel, and to educate them in the importance of securing and protecting both military and personal property.

A security education program, therefore, provides an excellent means of disseminating crime prevention information, and of encouraging the active participation of all personnel in observing and reporting security deficiencies, violations, or hazards of any nature.

3-9 Program of Instruction

a. The security manager is responsible for planning an effective program of instruction. Profitable use of the limited time normally available for such instruction demands the techniques of a competent instructor. The security manager should give the more important portions of the instruction. Other competent instructors may be used for less important phases or for phases which concern their areas of responsibility, training, and experience.

b. FM 30-17 provides an excellent discussion of the planning and implementation of a security education program. While the program outlined is directed primarily to intelligence security, a review will indicate many points at which physical security and crime prevention education can be integrated.

c. Each of the offices listed here can assist in the formulation of the program by contributing materials from its own areas of responsibility, knowledge, and interest. Each can also assist by presenting security briefings within those areas.

Staff judge advocate
Chaplain
Special services officer
Safety director
Information officer
Post surgeon
CID representative
Character guidance council representative
Major organizational command representatives
Local police and allied agencies

d. The program should be based on an evaluation of the total security posture of the installation. It should begin with an explanation of the program, its aims and objectives—the WHY.

e. It should then develop the necessary tools to reach those aims and objectives—the WHAT.

f. It should proceed to delineate methods of education by which the program will be conducted-through individual and group conferences, meetings, speeches, use of news media, posters, placards, leaflets, etc.—the HOW.

g. Each program must provide for initial and refresher training. It will also provide for debriefing of appropriate personnel upon their reassignment, retirement, departure on leave, and at other appropriate times.

h. The program must, above all, stress the absolute requirement for the support of every individual, regardless of any security clearance he mayor may not have, and regardless of his work assignment.

i. As a minimum, each program should include materials on any recent incidents of security deficiency or violation, and any areas of laxity or trends that have become

apparent in the security posture of the installation.

3-10 Scheduling and Testing

Frequent short periods of instruction are more effective than less frequent long periods. The ideas contained in four well-planned weekly 15-minute classes are more readily absorbed than those contained in a 1-hour lecture once a month-regardless of how well the latter is planned and delivered. Instruction that infringes on the free time of the audience is seldom well received. Short periods of instruction to selected groups are easier to schedule without disrupting the operation.

In any form of instruction, testing serves the dual purpose of keeping the audience alert and indicating the efficiency of the presentation and the total program. Tests do not necessarily involve written answers. In fact, skits and hypothetical situations tend to enliven the instruction. Audience participation in giving consequences or solutions to situations presented will accomplish the same results.

Personnel Movement Control



Perimeter barriers, intrusion detection devices and protective lighting provide physical security safeguards; however, they alone are not enough. A positive personnel movement control system must be established and maintained to preclude unauthorized entry, and to facilitate authorized entry at personnel control points. Access lists, personal recognition, security identification

cards and badges, badge exchange procedures, and personnel escorts contribute to the effectiveness of movement control systems.

The best control is provided when systems incorporate all these elements. Simple, understandable, and workable identification and movement control procedures should be used to achieve security objectives without impeding efficient operations. Properly organized and administered, a personnel and movement control system provides a means not only of positively identifying those who have the right and need to enter or leave an area, but also of detecting unauthorized personnel who attempt to gain entry.

Identification of Personnel — Section I

4-1 Purpose of Movement Control and Identification

a. Prevent introduction of harmful devices, materiel, or components.

b. Prevent misappropriation, pilferage, or compromise of materiel or recorded information by means of:

- Package
- Materiel
- Property Movement Control.

c. This prevention is accomplished through:

(1) Initially determining who has a valid requirement to be in an area.

(2) Limiting access to those persons who have that valid requirement.

(3) Establishing procedures for positive identification of persons within, and of persons authorized access into, areas.

(4) Issuing special identification cards or badges to personnel authorized access into restricted areas.

(5) Using access lists.

(6) Using identification codes.

(7) Using duress codes

4-2 Employee Screening

a. Screening job applicants and employees to eliminate potential espionage and sabotage agents and other security risks is important in peacetime and is extremely important in time of a national defense emergency. For such screening to be most effective, it should be incorporated into standard personnel policies for peacetime as well as for times of emergency.

b. Personnel Security Survey Questionnaire. The use of a personnel security questionnaire is essential in the investigation of both applicants and employees. The security questionnaire should be screened for completeness and, in the case of applicants, obvious undesirables eliminated from further consideration. A careful investigation should be conducted to assure that the applicant's or employee's character, associations, and suitability for employment are satisfactory.

c. Sources of Data. The following

sources may be helpful in securing employment investigative data:

(1) State and local police, to include national and local police in overseas areas.

(2) Former employers.

(3) References (including those not furnished by applicant or employee. These are known as throw-offs, and their names are obtained during interviews of references furnished by applicants or employees).

(4) Public records.

(5) Credit agencies.

(6) Schools (all levels).

(7) Others as appropriate. (These may include the FBI, the US Army Criminal Records Repository, etc.). In requesting investigative data from any of the above sources, enough information should be furnished to properly identify the applicant or employee and avoid error in identity.

4-3 Identification System

a. An identification (ID) system should be established at each installation or facility to provide a means of identifying all military personnel, civilian employees, and visitors. The system should provide for the use of security identification cards or badges to aid in control and movement of personnel into, within, and out of specified areas or activities.

b. The standard identification media, DD Form 2A (Military) or DA Form 1602 (Civilian Employee), may be prescribed for personnel by installation or facility commanders as valid identification for access to areas that are basically administrative in nature, contain no security interest, and are not in the restricted area category.

c. Personnel requiring access to restricted areas should be issued a security identification card or badge as prescribed in AR 606-5. The identification card or badge should be designed as simply as possible and still provide for adequate control of the movement of personnel.

d. Provisions for identification by card or badge control at an installation or facility should be included as part of the physical security plan.

4-4 Use of Identification Media

a. Designation of the various areas where media are required.

b. Description of the various types in use plus authorizations and limitations placed upon the holder.

c. Required presentation at times of entering and leaving each area, including nonoperational hours.

d. Details, of where, when, and how worn, displayed, or carried.

e. Procedures to be followed in case of loss or damage.

f. Disposition on termination of employment or as a result of investigations and personnel actions.

g. Prerequisites for reissue.

4-5 Types of Systems

Most Common Identification Systems

- ☐ Single card or badge
- ☐ Card or badge exchange
- ☐ Multiple cards or badges

4-6 Card and Badge System

a. A security identification card or badge system should be established to admit and control the movement of all persons admitted to restricted areas employing 30 or more persons per shift. However, the commander may at his discretion authorize a card or badge system in restricted areas where less than 30 persons per shift are employed.

b. Of the several identification systems used in access control, three of the most commonly used are the **single card or badge system,** the **card or badge exchange system,** and the **multiple card or badge system.** These ID systems may be used either for cards carried on the person or for cards or badges worn on outer clothing.

c. A system may be established (in an appropriate situation) for issuance of identification cards or badges at the main entrance to an installation. Such a system can be used for visitors and similar personnel.

4-7 Single Card or Badge

a. With this system, permission to enter specific areas is shown by letters, numerals, or colors. It has a major limitation-loose control. The opportunity for alteration or duplication is high.

b. This system gives comparatively loose control and is not recommended for security areas. Permission to enter does not always go with the need to know, and the fact that ID cards and badges frequently remain in the bearer's possession during off duty or off post hours gives the opportunity for alteration or duplication.

4-8 Card or Badge Exchange

a. In this system, two items contain identical photographs but different background colors, or one item has an overprint. One is presented at the entrance to a specific area and exchanged for the other, which is carried or worn while in that area. Individual possession upon issuance is only in the area, to **decrease the possibility of forgery or alteration.**

b. This method provides extra security by having both photographs identical. In this type of system, the second badge or card is kept in the security area and never leaves the area.

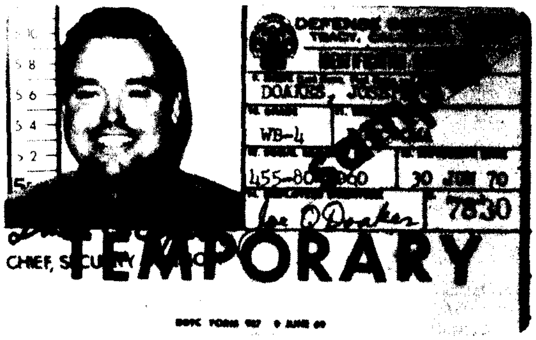
4-9 Multiple Card or Badge

a. Instead of having specific markings on the ID card or badge denoting permission to enter various restricted areas, the multiple card or badge system makes an exchange at the entrance to each security area within the installation. Exchange cards or badges are kept at each area for only those individuals who have the appropriate card or badge. By virtue of the localized and controlled exchange requirements, this is the most secure and effective system.

b. Card and badge data are identical and must be so to allow comparisons.

4-10 Card and Badge Specifications

a. Security ID cards and badges should be of a type of design and construction which will make them, for all practical purposes, tamperproof, and which will meet the requirements of AR 606-5.



b. Security ID card and badge inserts should be prenumbered to avoid any possibility of reissuing any number. Acquisition, storage, and control of card and badge components and all engraved plates must be accomplisher as prescribed in AR 606-5.

c. Issuance and Accountability:

(1) Identification card or badge issuance, accuntability, and control should be accomplished at a central office, preferably the office of the provost marshal or physical security office, so a minimum of time me elapses between change in the status of a card or badge and noti fication of the security forces.

(2) A duplicate of each issued card or badge and a file on each hearer should be kept including, in addition to the data entered on the card or badge, the bearer's residential address and telephone number.

(3) Why such strict control?

(a) Because any ID card or badge may be altered or reproduced by a person having the time and sufficient skill in printing. engraving and photocopying, the makeup, issuance, and accountability of cards and badges must be fully controlled.

(b) Because control commences with the manufacturer or supplier.

(c) When inserts or complete cards or badges are secured commerically, verification should be made that adequate control is exercised by the supplier. This is especially important when engraving or special paper is concerned.

4-11 Enforcement Measures

The most vulnerable link in any identification system is its enforcement. Perfunctory performance of duty by the security forces in comparing the bearer with the card or badge may weaken or destroy the effects of the most elaborate system. Positive enforcement measures should be prescribed to insure effective operation of the personnel and identification system. These should include, but not be limited to the following:

a. Security personnel designated for duty at entrance control points should be chosen for their alertness, quick perception, tact, and good judgment.

b. Formalized, standard procedures for conducting assemblies, posting, and relief of personnel, and frequent inspection of personnel on post at irregular times are effective means to preclude posting of unqualified personnel and perfunctory performance of duty.

c. A uniform method of handling or wearing security ID cards or badges should be prescribed. If carried on the person, the card must be removed from the wallet or other container and handed to security personnel. A badge should be worn in a con spicuous position to expedite inspection and recognition from a distance.

d. Entrances and exits of restricted areas should be arranged so that arriving and departing personnel arc forced to pass in a single file in front of security personnel. In some instances, the use of turnstiles may be advisable to assist in maintaining positive control of entrance and exit.

e. Artificial lighting at the control points should be arranged so that it illuminates the arriving and departing personnel

and should be of sufficient intensity to enable security personnel to compare and identify the bearer with the ID card or badge.

f. Enforcement of access control systems rests primarily on the installation security forces. However, it is essential that they have the full cooperation of the employees, who should be educated and encouraged to assume this security responsibility. Employees should be instructed to consider each unidentified or improperly identified individual as a trespasser. In restricted areas where access is limited to particular zones, employees should report movement of individuals to unauthorized zones.

g. Identification card and badge racks or containers used at control points for an exchange system should be positioned so they are accessible only to guard personnel.

h. A responsible custodian should be appointed by competent authority to accomplish control procedures required by AR 606-5 for issue, turn in, recovery, or expiration of security ID cards and badages, The degree of compromise tolerable in the identification system is in direct proportion to the degree of security required or indicated. The following control procedures are recommended for preserving the integrity of a card and badge system:

(1) Maintenance of an accurate written record or log listing, by serial number, all cards and badges, showing those on hand, to whom issued, and disposition (lost, mutilated, or destroyed).

(2) Authentication of records and logs by the custodian.

(3) Periodic inventory of records by a commissioned officer.

(4) Prompt invalidation of lost cards and badges.

(5) Conspicuous posting at security control points of current lists of lost or invalidated cards and badges.

(6) Establishment of controls within re stricted areas to enable security personnel on duty to determine promptly and accurately the number of persons within the area at any time.

(7) Establishment of a two-man rule when required.

(8) Establishment of procedures to control movement of visitors to security areas. A visitor control record should be maintained and located where positive controls can be exercised.

4-12 Visitor Identification And Control

a. Physical security precaution against pilferage, espionage, and sabotage requires screening, identification, and control of visitors. Visitors are generally in the following categories:

(1) Persons with whom every installation or facility must have dealings in connection with the conduct of its business, such as representatives of suppliers, customers, licensers or licensee, insurance inspectors or adjusters, government inspectors (national, state, and local), service industry representatives, contractors, employees, etc.

(2) Individuals or groups who desire to visit an installation or facility for a purpose not essential to, or necessarily in furtherance of, the operations of the installation or facility concerned. Such visits may be desired, for example, by business, educational, technical, or scientific organizations and individuals or groups desiring to further their particular interests.

(3) Individuals or groups specifically sponsored by government agency organi-

zations such as foreign nationals visiting under technical cooperation programs and similar visits by US nationals. Requests for visits by foreign nationals should be processed in accordance with AR 380-25.

(4) Individuals and groups who the government generally encourages but does not specifically sponsor, because of the contribution they make to economic and technical progress or to defense production in the United States and/or in friendly nations.

(5) Guided tour visits to selected portions of installations in the interest of public relations.

(6) Further information concerning requirements and procedures for visits will be found in AR 381-130 and AR 550-50.

b. Arrangements for identification and control of visitors may include the following:

(1) Positive methods of establishing the authority for admission of visitors, as well as any limitations relative to access.

(2) Positive ID of visitors by means of personal recognition, visitor permit, or other identifying credentials. The employee, supervisor or officer in charge should be contacted to ascertain the validity of the visit.

(3) Availability and use of visitor registration forms and records that will provide a record of identity of the visitor, time and duration of his visit, and other pertinent control data.

(4) Availability and use of visitor ID cards or badges. Such identification media should be numbered serially and indicate the following:

(a) Bearer's name.
(b) Area or areas to which access is authorized.
(c) Escort requirements, if any.
(d) Time limit for which issued.
(e) Signature (or facsimile).
(f) Photograph, if desired and available.

(5) Procedures which will insure supporting personal identification in addition to check of visitor cards or badges at restricted area entrances.

(6) Procedures for escorting visitors having limitations relative to access through areas where an uncontrolled visitor, even though conspicuously identified, could acquire information for which he is not authorized. Foreign national visitors should be escorted at all times.

(7) Controls which will recover visitor ID cards or badges on expiration, or when no longer required.

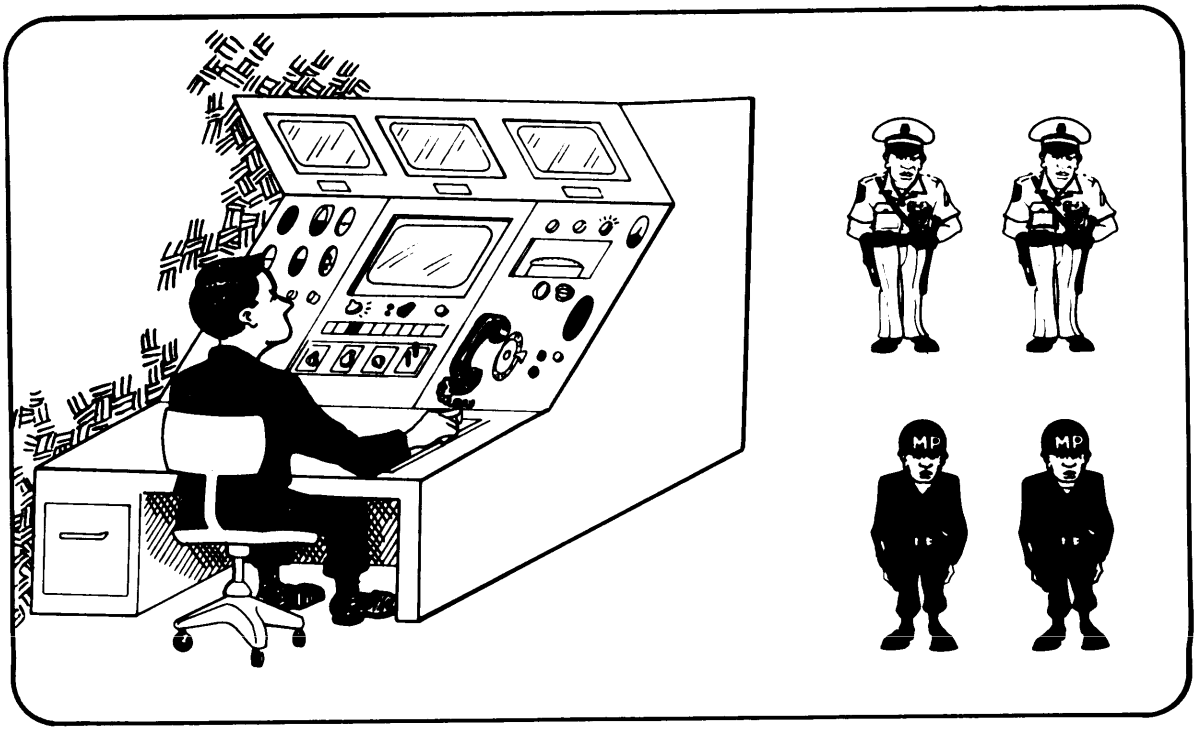
(8) Twenty-four hour advance approval when possible. Where appropriate, the installation should prepare an agenda for the visit and designate an escort officer.

4-13 Sign/Countersign And Codeword

This additional measure to verify identity is primarily used in tactical maneuvers and during Army Training and Evaluation Programs (ARTEP). The sign/countersign or codeword procedure should be checked and tested to insure immediate change if. compromised.

4-14 Duress Code

This is a simple word or phrase used during normal conversation. It alerts other security personnel that an authorized person has been forced to vouch for an unauthorized individual. A viable duress code requires preplanning to insure appropriate response. And it is changed frequently to minimize compromise.



Equipment And/Or Manpower

This system assists in the control of entry and departure of personnel to and from these areas and provides a strict control and identification system within the area.

4-15 Use of Escorts

Escorts must be chosen because of their ability to accomplish tasks properly and effective y and their knowledge of areas to be visited, to include all security requirement.

a. Each should be a representative of the person or activity visited.

b. Escort personnel should be other than military police or civilian guards.

c. Whether or not the escort remains with such visitor during the time he is within the restricted area is determined by local regulations. Personnel listed on the access list may be admitted to restricted areas without escort, depending upon local policy.

4-16 Entry Roster

Admission of unit or installation personnel to restricted areas should be granted only to those positively identified

and whose names appear on a properly authenticated roster of all persons authorized by competent authority to enter.

a. Each time a permanent addition or deletion is made, this correction can initially be accomplished by pen and ink.

b. Changes may be published in the same manner as the original roster.

c. Rosters should be maintained at access control points to facilitate positive control and be kept current, verified, authenticated, and accounted for by an individual designated by the commander. Admission of persons other than those on the authorized roster should be subject to specific approval by the installation or facility commander, or his designated representative. Such persons will be escorted or supervised.

4-17 Two-man Rule

a. At least two authorized persons, each capable of detecting incorrect or unauthorized procedures with respect to the task being performed and who are familiar with applicable safety and security requirements, will be present during any operation that affords access to sensitive weapons.

b. The rule is designed to prohibit access to sensitive weapons by a lone individual. Two authorized persons will be considered to be present when they are in a physical position from which they can positively detect incorrect or unauthorized procedures with respect to the task and/or operation being performed. When application of the two-man rule is required, it will be enforced constantly by the persons who constitute the team while they are accomplishing the task or operation assigned and until they leave the area in which it is required.

c. The two-man rule should not, however, be considered applicable only in the cited situations. It can, and should, be applied in many other aspects of physical security operations, such as the following:

(1) When uncontrolled access to vital machinery, equipment, or materiel might provide opportunity for intentional or unintentional damage which could affect the mission or operation of the installation or facility.

(2) Where uncontrolled access to funds could provide opportunity for diversion by falsification of accounts.

(3) When uncontrolled delivery or receipt for materials could provide opportunity for pilferage through "short" deliveries and false receipts.

(4) When uncontrolled access to an arms or ammunition storage room could provide an opportunity for theft. Keys should be issued so as to require the presence of at least two men to unlock the three locks required under provisions of AR 190-11. (This is analogous to the safe deposit box system, which requires two keys in the possession of two different persons.)

d. The foregoing are only a few examples the listing is virtually limitless. The important point to be stressed is that the provost marshal and the physical security manager should explore every possible aspect of physical security operations in which the two-man rule would provide additional security and assurance, and include all appropriate recommendations and provisions in the overall physical security plan.

4-18 Additional Procedures For Specific Groups

a. Visitors— Entrance prerequisites:

(1) Verify identity.

(2) Contact person or activity to be visited to insure identity and validity of visit.

(3) Record visitor information.

(a) Issue visitor badges.
(b) Use registration forms.

b. VIPs and foreign nationals, special consideration— Coordination with protocol office:

(1) Twenty-four hour advance notice desirable.

(2) Agenda for visit and designation of escort officer, if appropriate.

c. Civilians working on jobs under government contract— The security manager should:

- Coordinate with procurement office to determine applicable provisions of contract.
- Identify procedures to control the movement of those employees.
- Insure that protection of the construction site is accomplished with available resources.

d. Supervisors using cleaning teams should seek technical advice from the physical security office on internal controls for each specific building.

e. Public utility and commercial service representatives:

(1) Entrance prerequisites same as for visitors.

(2) Designated activity personnel check on authority to remove equipment for maintenance.

f. DOD employees in work areas after normal operational hours:

☐ Supervisors establish internal controls, based on coordination with the security manager.

☐ Notify security personnel of workers' presence and expected duration of work.

4-19 Security Personnel At Entry and Exit Points

The security manager responsible for these individuals must insure that the personnel:

a. Are alert, very perceptive, tactful, and capable of exercising sound judgment in executing their duties and responsibilities.

b. Conduct frequent, irregular checks of their assigned areas during periods of inactivity (holidays, weekends, after-duty hours, etc.). (Also, see chapter 5.)

4-20 Mechanized/Automated Systems

Identification and access control systems base their identification judgment factor on a remote capability through a routine discriminating device for positive ID, as opposed to the manual system's using a guard force member to conduct identification based on access rosters and personal recognition.

a. In a mechanized identification system, the following actions occur within the machine:

(1) Receives physical ID data from an individual.

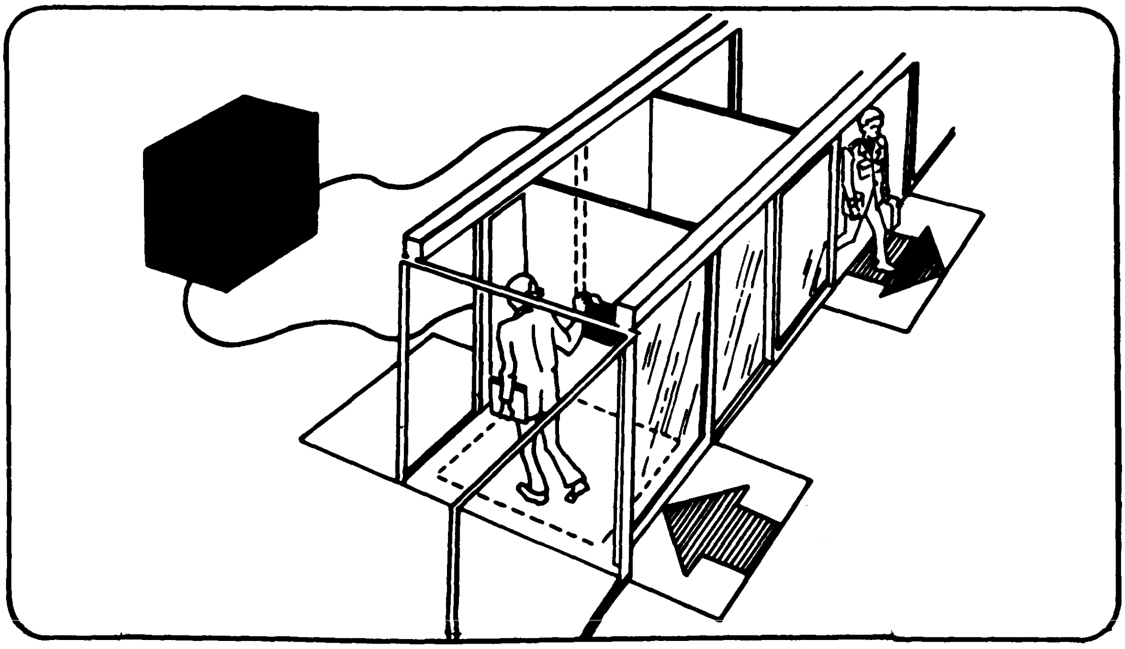
(2) Encodes this data for use.

(3) Compares this data to stored data.

(4) Makes ago or no go decision based on the comparison.

(5) Translates the results into readable form.

b. Several mechanical devices add to the security posture and are expanding in popu-



Computer makes go or no go decision based on data received.

larity and use. Such devices use the following techniques:

(1) Magnetic coding.

(2) Embossing.

(3) Optical characters.

(4) Dielectric coding.

c. Specialized mechanical systems are ideal for highly sensitive situations because these systems use a controlled process in a controlled environment to establish the required data base and accuracy.

(1) One innovative technique with application to identification and admittance procedures involves dimension comparisons. The dimension of a person's full hand is compared to previously stored data to determine entry authorization. Another specialized machine reader can scan a single fingerprint and provide positive identification of anyone attempting entry. (Good for semiremote environment.)

(2) The voiceprint technique is being widely used as an identification means and features rapid processing with accuracy.

d. An all-inclusive automated ID and access control system reinforces the security indepth ring through its easy and rapid change capability. The computer is able to do this through its memory, stored on magnetic tape or disc. Changes can be made by remote use of specific code numbers. The big advantage for this system is that changes do not require wiring or media alterations.

e. The commercial security market has a wide range of mechanized and automated hardware-software systems interfacing for the enhancement of any security posture. Assessment of security needs and use of the planning, programing and budgeting procedures outlined in chapter 2 will greatly assist a security manager in improving the overall security posture.

Designation of Restricted Areas

4-21 Restricted Areas

The term "restricted area" as used here, is defined (AR 380-20) as "Any area, access to which is subject to special restrictions or controls for reasons of security or safeguarding of property or material."

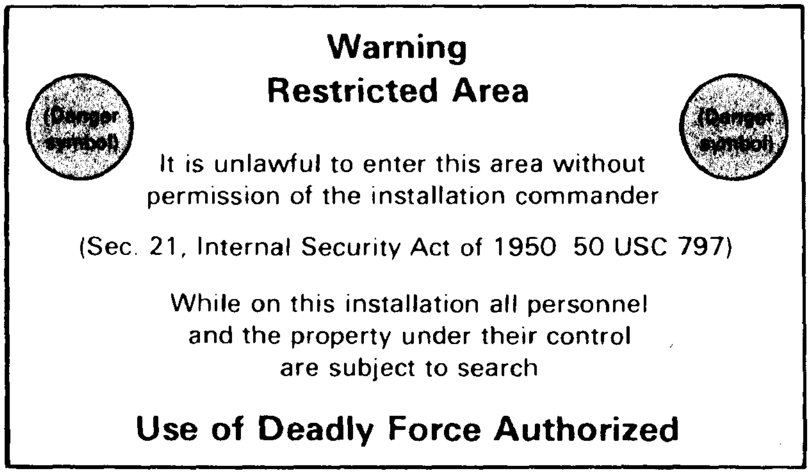
a. Designation and establishment of restricted areas is the responsibility of the military commander of the installation or facility. His authority is derived from Department of Defense Directive No. 5200.8, dated 20 August 1954, which was issued pursuant to the provisions of section 21, Internal y y Act of 1950. Within the Army, the DOD Directive was implemented by AR 380-20.

b. AR 380-20 states, "these regulations apply only to Army installations or activities within the continental United States. Oversea commanders may utilize these regulations for guidance in establishing local procedures."

c. The terms, "restricted area," "controlled area," "limited area," and "exclusion area," are described by AR 50-5 as standard terminology. The regulation states that these terms "will be employed wherever United States Army nuclear weapon material is involved." Such employment outside the continental United States would, however, require publication of an appropriate command directive, since AR 380-20 would not apply.

d. It is clearly the meaning and intent of these documents that the security protection afforded by a restricted area pertains particularly to subversive activities control, that is, protection against espionage, sabotage, or any such actions adversely affecting the national defense of the United States. Within this context, the designation "restricted area," as defined, is not applicable to an area solely for protection against common pilferage or misappropriation of property or material which is not classified or not essential to the national defense. For example, an area devoted to the storage or use of classified documents, equipment or materials should be so designated to safeguard against espionage. An installation communications center should also be so designated, to safeguard against sabotage. On the other hand, a cashier's cage or an ordinary mechanic's toolroom should not be so designated, although the commander may impose controls on access thereto. This may be as simple a matter as posting a sign, "Off Limits to Unauthorized Personnel," or it may require the erection of fences, railings, etc. The responsibility for designation is, of course, the commanders. However, in furnishing advice to him, the provost marshal or physical security manager should consider carefully the foregoing guidance; evaluate the purpose of any proposed or necessary designation of a restricted area; coordinate with the intelligence officer and staff judge advocate; and formulate his recommendations accordingly.

e. To comply with the requirements of the Internal Security Act of 1950 and the provisions of implementing directives, and to



provide for proper procedures in cases of violation, a restricted area must be designated in writing as such by the military commander and must he posted with warning signs or notices of the type described in AR 380-20. 0-20.

f. The establishment of restricted areas improves security by providing defense in depth (see also paragraph 1- 3c) and increases efficiency by providing degrees of security compatible with operational requirements. These specially designated areas may also provide for economy of operation by reducing the need for stringent control measures for the installation or facility as a whole.

4-22 Types of Restricted Areas

a. The degree of security and controls required depends upon the nature, sensitivity. or importance of the security interest or other matter involved. Restricted areas may be established to provide the following:

(1) Effective application of necessary security measures and exclusion of unauthorized personnel.

(2) Intensified controls over those areas requiring special protection.

(3) Conditions for compartmentalization of classified information or critical equipment or materials, with minimum impact on operations.

b. Different areas involve different degrees of security interest, depending upon their purpose and nature of work, information, and/or materials concerned. For similar reasons, different areas within an installation may have varying degrees of importance. In some cases, the entire area of an installation may have a uniform degree of importance, requiring only one level of restriction and control. In others, differences in degrees of importance will require further segregation or compartmentalization of activities.

c. To meet these different levels of sensitivity and to provide for an effective and efficient basis for applying the varying degrees of restriction of access, control of movement, and type of protection required, restricted areas or portions thereof may be further administratively designated as "exclusion," "limited," or "controlled" areas. It must be understood that the term "restricted area" is in effect a legal designation (Internal Security Act of 1950), whereas the terms, "exclusion" and "limited" are administrative only (AR 380-20). The term "controlled area, " is not mentioned in either the Security Act or

AR 380-20, and is used only as a matter of convenience.

d. The primary criteria for administrative designation of exclusion, limited, and controlled areas is the degree of restriction or controls required to prevent compromise of the security interest or other matter therein. Characteristics of these areas are:

(1) Exclusion area— A restricted area containing one of the following:

(a) A security interest or other matter of such nature that access to the area constitutes, for all practical purposes, access to such security interest or matter.

(b) A security interest or other matter of such vital importance that proximity resulting from access to the area is treated as equivalent to **(a)** above.

(2) Limited area— A restricted area containing a security interest or other matter and in which uncontrolled movement will permit access to such security interest or matter, but within which access may be prevented by escort and other internal restrictions and controls. Individuals who have a legitimate reason for entering a limited area may do so if internal restrictions and controls are provided to prevent access to the security interest or other matter. These measures usually consist of escorts and other physical safeguards.

(3) Controlled area— An area, usually adjacent to or encompassing limited or exclusion areas. Access to a controlled area is restricted to those with a need for access. However, movement of authorized personnel within this area is not necessarily controlled, since mere access to the area does not provide access to the security interest or other matter within the exclusion or limited areas. The controlled area is provided for administrative control, safety, and/or as a buffer zone for depth in security for the exclusion or limited areas. The degree of control of movement within this area will, therefore, be as prescribed by the appropriate commander.

e. You can see from the foregoing that an installation may have varying degrees of security designation, or none at all. It maybe designated in its entirety as a restricted area, with no further degree of restrictions or controls. It may, however, provided that it is first designated as a restricted area, to bring it under the provisions of the Internal Security Act of 1950, be further administratively classified, in whole or in portions, as an exclusion area, limited area, or controlled area with specific clear zones (figures 6,7,8,9 and 10).

4-23 Other Considerations

a. There are other important considerations which should be kept in mind concerning restricted areas and their compartmentalization. Some of these are:

(1) Immediate and anticipated needs can be determined by survey and analysis of the installation or facility, its missions, and the security interests or other matters on hand which require protection. Anticipated needs can be determined from future plans.

(2) The **nature of the security interest** or other matter to be protected. Classified documents and small items may be protected by securing them in safes or locked containers, whereas large items may have to be placed within guarded enclosures.

(3) Some **security interests are more sensitive to compromise** than others. Brief observation or a simple act by an untrained person may constitute a compromise in some cases. In others, detailed study and planned action by an expert may be required.

(4) All security interests should be **evaluated according to their relative importance.** This may be indicated by a

security classification such as TOP SECRET, SECRET, or CONFIDENTIAL, or by their criticality. That is, the effect their loss or compromise would have on national defense or the mission of the installation or facility.

b. Parking areas for privately owned vehicles must be established outside restricted areas, if at all possible. This is due to the fact that large amounts of articles can be readily concealed in vehicles, and would then be harder to detect than if they were on a person. Also, entrances should be kept at a minimum necessary for safe and efficient operation and control.

c. Establishment of restricted areas within an installation improves overall security by providing security in depth. Limited and exclusion areas serve as inner rings of security; the controlled area serves as a buffer zone. As a general rule, an increase in security results in some slowdown in operations. However, **without security there may be no operations.** The use of security areas makes it possible to have security compatible with operational requirements. Instead of establishing stringent control measures for the installation as a whole varying degrees of security can be provided as required and as conditions warrant. In this way, interference with overall operations is reduced to a minimum and operational efficiency can be maintained at a relatively high level.

d. Where required, adequate physical safeguards such as fences, gates, and window bars must be installed to deny entry of unauthorized persons into restricted areas. Except where such action would tend to advertise an otherwise concealed area, warning signs or notices must be posted in conspicuous and appropriate places, such as ordinary entrances or approaches to these areas, and on perimeter fences or boundaries of each area.

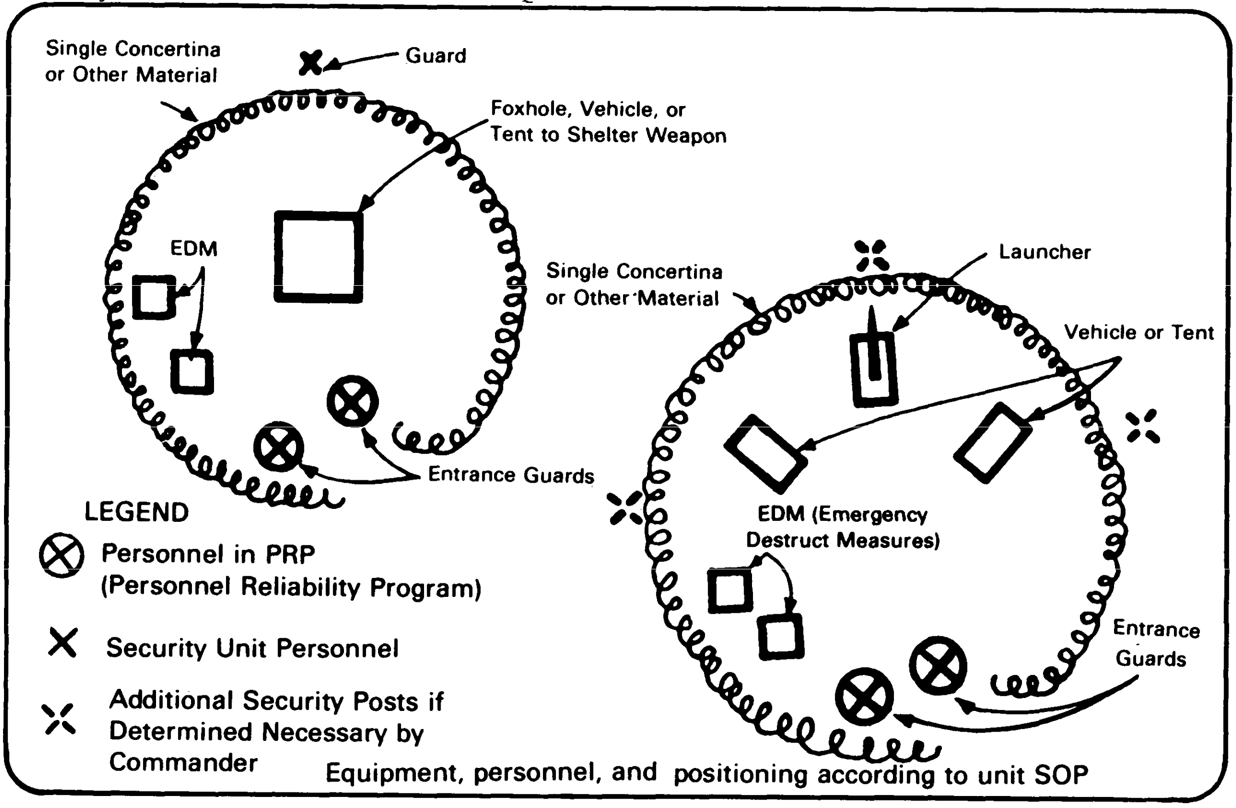
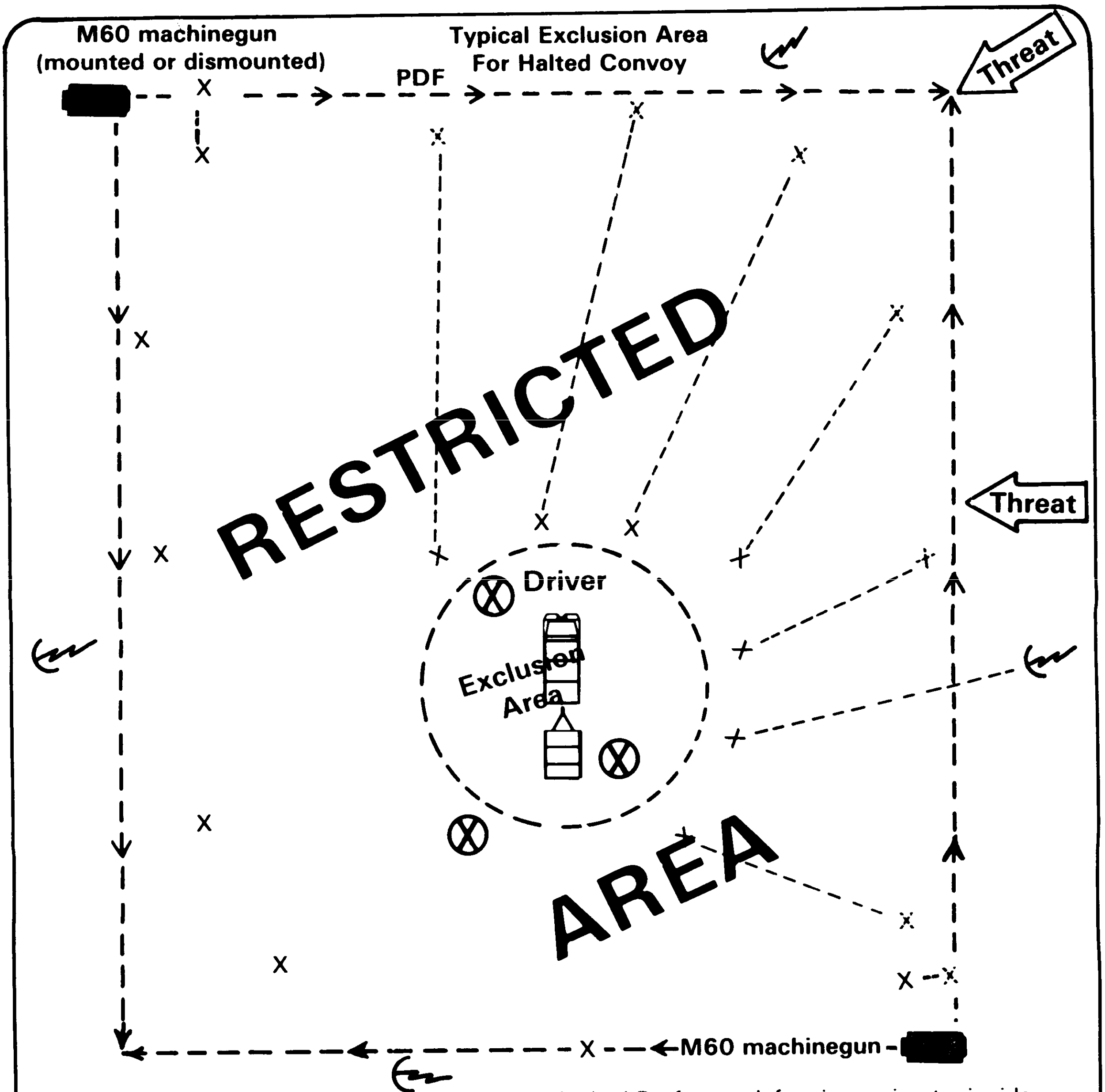


Figure 6—Sample layout of temporary tactical restricted areas.



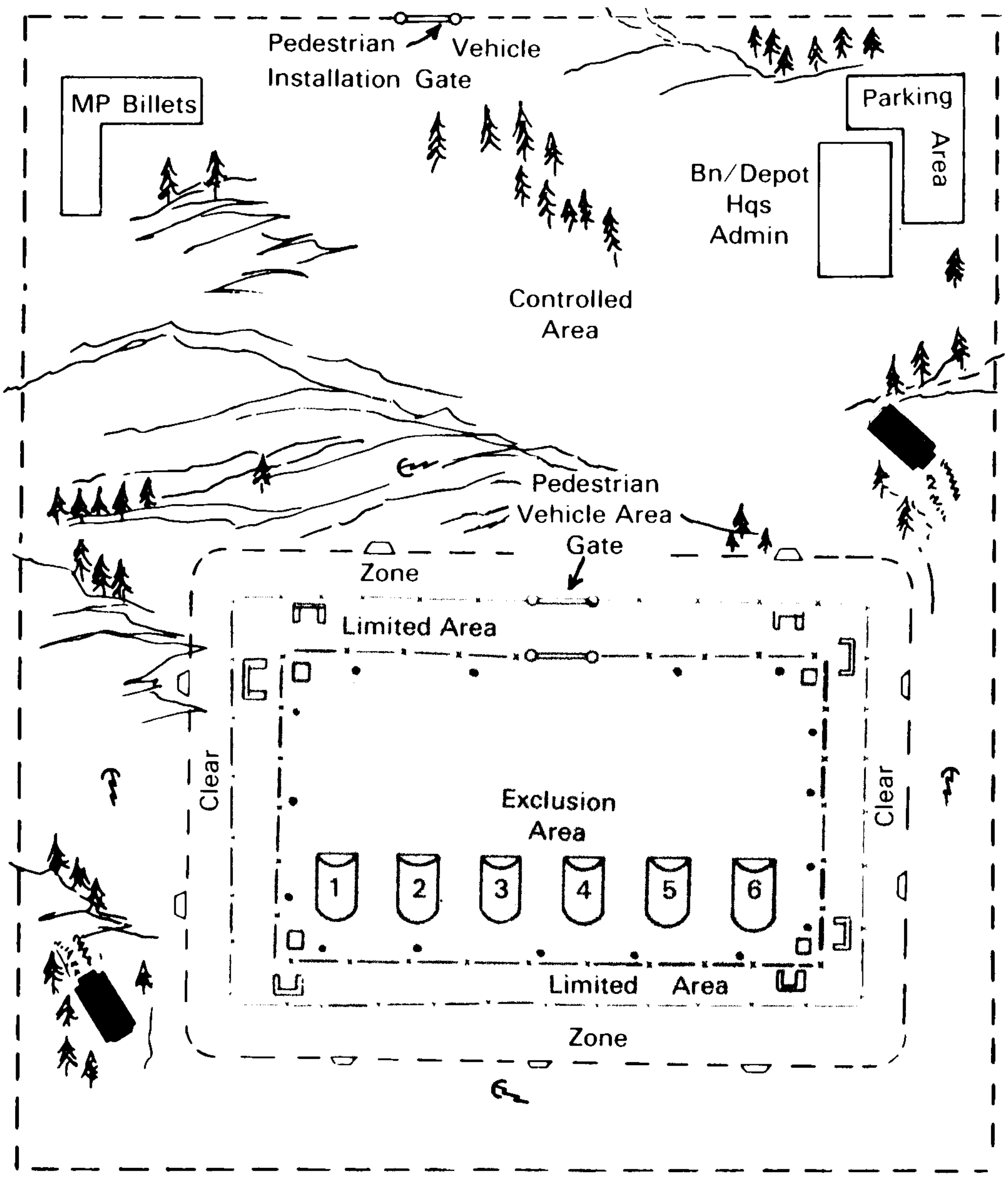
Note: Other vehicles and personnel, to include the LPs, form a defensive perimeter inside the primary directions of fire of the M60 machineguns. During attack, alternate machinegun crews should be placed in the perimeter away from primary machineguns and be spaced so that if they are needed as replacements, large gaps do not appear in the perimeter.

Legend

- X — MP rifleman
- ⊗ — PRP qualified (see AR 50-5)
- ←–←– — Principal direction of fire
- ◌ — Temporary exclusion area (size depends on terrain and threat force)
- Listening Post

Figure 7—Sample layout for temporary tactical exclusion area.

Depot Complex
(Restricted Area—Base Defense)



- - - - Chainlink fencing with top guard on perimeter of restricted area

Legend

- ☐ Guard tower
- Listening post
- ● Protective lighting
- Fighting position
- Restricted area warning signs
- MG Depending on direction of attack and terrain features, the MG teams may displace to establish final protective fires (FPF) or principal direction of fire (PDF).

Figure 8—Diagram of depot complex example.

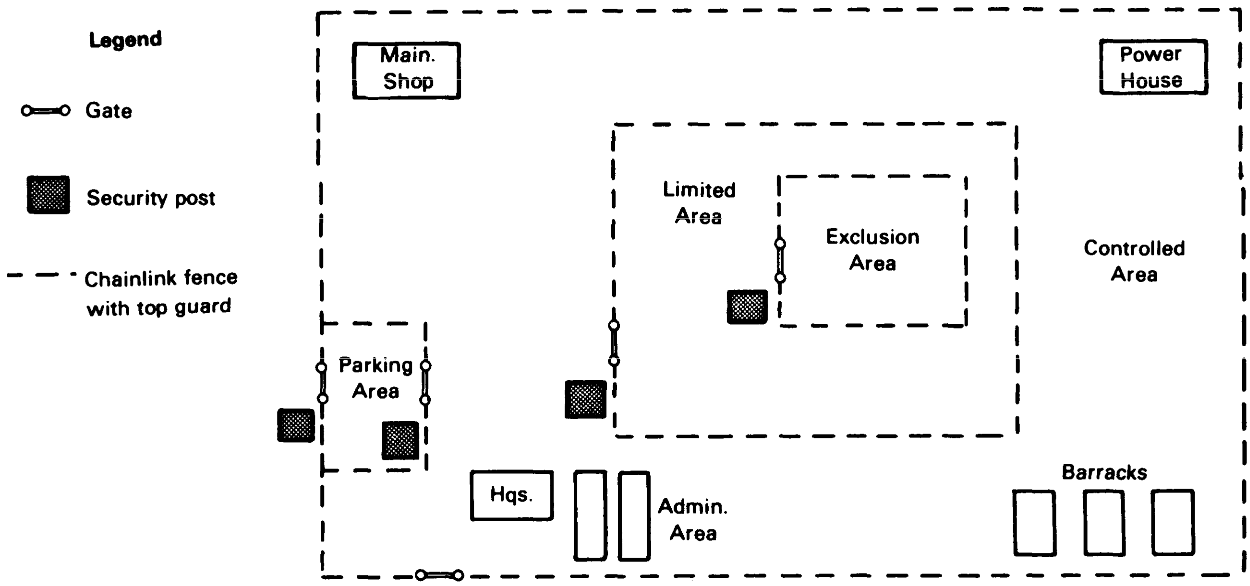


Figure 9—Schematic diagram of simplified restricted area and degrees of security.

Package, Materiel, and Property Control Section IV

4-24 Package Control

a. A good package control system helps prevent or minimize pilferage, sabotage and espionage. Only packages with proper authorization should be permitted into restricted areas without inspection.

b. A positive system should be established to control movement of packages, materiel, and property into and out of the installation.

c. A package checking system, using Individual Property Pass, DA Form 1818, or a similar form, may be used at the entrance gate for the convenience of employees and visitors. When practicable, inspect all outgoing packages except those properly authorized for removal. When 100 percent inspection is impracticable, conduct frequent unannounced spot checks.

4-25 Property Controls

a. Property controls must not be limited to packages carried openly; but must include control of anything that could be used to secret property or materiel of any type.

b. Persons should not be routinely searched except in unusual situations. When they are, it should be only in accordance with published command directives.

4-26 Vehicle Control

a. All privately owned/visitor-operated motor vehicles on the installation should be registered with the provost marshal or the installation physical security office. Requirement to display a tag or decal should be IAW AR 190-5 and AR 210-10.

b. Vehicles belonging to visitors should be identified by a temporary decal or identification media different from permanent registration to permit ready recognition by security personnel.

c. When authorized vehicles enter or exit a restricted area, each must undergo a **sys-**

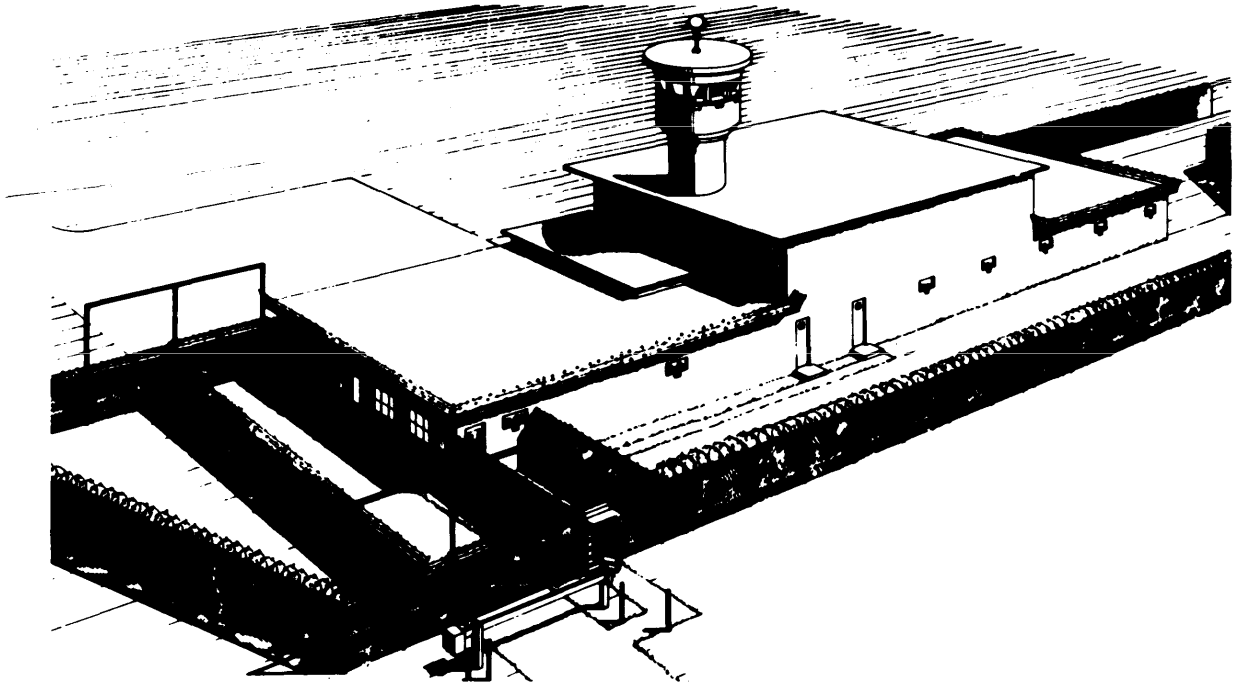


Figure 10—Drawing of standard physical security layout.

tematic search, including, but not limited to, the following areas:

- Interior of vehicle
- Engine compartment
- External air breathers
- Top of vehicle
- Battery box
- Cargo compartment
- Undercarriage.

4-27 Truck and Railroad Car Control

a. Movement of trucks and railroad cars into and out of installations or facilities should be supervised and each inspected to prevent the entry or removal of unauthorized persons or materiel. Inspectors should be especially watchful for explosives or incendiaries.

b. Truck and railroad entrances should be **controlled by locked gates** when not in use, and should be under security supervision when unlocked or opened for passage.

c. **Identification cards or badges** should be issued to operators of trucks and railroad engines to insure proper identification and registration of those entering and leaving the area. Such cards or badges should permit access only to specific loading and unloading areas.

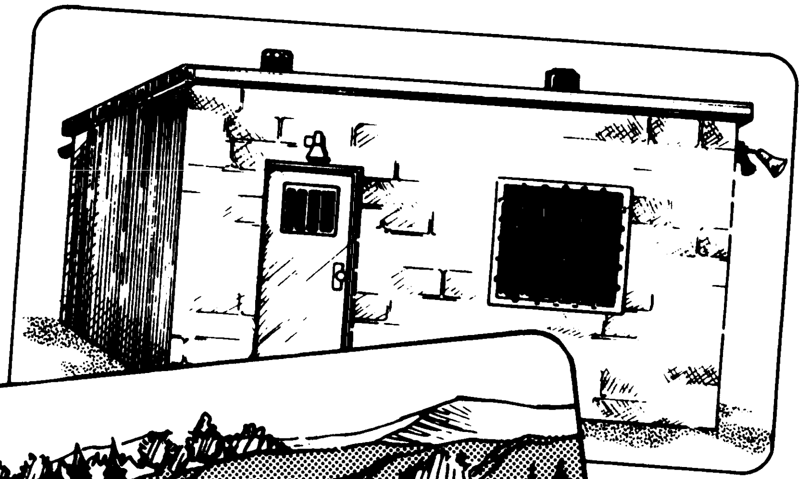
d. All conveyances entering or leaving a protected area should be required to pass through a service gate manned by security forces. Drivers, helpers, passengers, and vehicle contents should be carefully examined. The security check should include

- Appropriate entries in security log, date, operator's name, description of load, time entered and departed.
- License check of operator.
- Verify seal number with shipping document and examine seal for tampering.

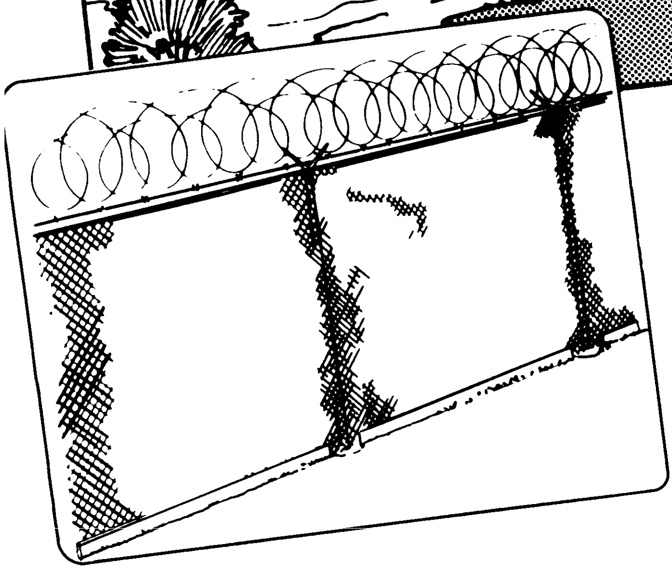
e. Incoming **trucks and railroad cars must be assigned escorts before they are permitted to enter designated limited or exclusion areas.** Commanders should establish published procedures to control the movement of trucks and railroad cars that enter designated **restricted areas** to discharge or pick up cargo. Escorts should be provided when necessary.

Chapter 5

Protective Barriers







Protective barriers are used to define the physical limits of an installation, activity or area and are used to restrict, channel or impede access.

Protective barriers are divided into two major categories—structural and natural. Natural protective barriers may be moun-deserts, or other terrain difficult to traverse. Structural protective barriers involve man-made devices such as fences, walls, floors, roofs, grills, bars, roadblocks or other construction to make penetration difficult.

5-1 Benefits

The use of barriers offers two important benefits to a physical security posture. First, they create a psychological consideration for anyone thinking of unauthorized entry. Second, barriers have a direct impact on the number of security posts needed and on the frequency of use for each post.

5-2 Considerations

Protective physical barriers should be used in the protection of the entire installation or facility and in establishing restricted areas. The following guidance may be used for protective structural barriers and the types of areas they serve:

a. The size of an area, which in some cases may embrace extensive tracts of land, will depend upon the nature of the security considerations. These considerations will have a bearing on the essentiality and cost effectiveness of establishing structural barriers on the outer perimeter. You can define the outer perimeter of a restricted area by:

(1) Structural barriers at control points and other points of possible entrance and exit.

(2) Natural or structural barriers between control points that are sufficiently obstructive and difficult to traverse—to control and to preclude accidental intrusion.

b. The size of a restricted area will depend on the degree of compartmentalization required and the complexity of the area. As a rule, size should be kept to a minimum consistent with operational efficiency. Positive barriers should be established for:

(1) Controlling vehicular and pedestrian traffic flow.

(2) Checking identification of personnel entering or departing.

(3) Defining a buffer zone for more highly classified areas.

5-3 Positive Barriers

Positive barriers should be designed in view of the threat, to deter access to the maximum extent.

a. Positive barriers are required for the entire perimeter of controlled, limited, or exclusion areas (see chapter 5). Specific types of barriers cannot be predesignated for all situations; however, they should incorporate the following elements:

(1) Structural perimeter barriers, such as fences, walls, etc.

(2) Provisions at points of entrance and exit for identification checks by either pass and badge exchange or badge examination (chapter 4).

(3) Opaque barriers to preclude visual compromise by unauthorized personnel may be necessary in certain instances.

b. When the greatest degree of security is essential, additional structural barriers may be required. Two lines of structural barriers should be installed on the perimeter; such lines of barriers should be separated by not less than 15 feet and not more than 150 feet for optimum enforcement, protection, and control.

c. If the nature of a secure area dictates a requirement for a limited or exclusion area on a temporary or infrequent basis, you may not be able to use the types of physical structural perimeter barriers described in paragraph 5-3a. In such cases, a temporary limited area or exclusion area may be established in which the lack of proper physical barriers is compensated for by additional security posts, patrols, and other security measures during the period of restriction (chapter 4).

5-4 Fence Design Criteria

Four types of fencing authorized for use in protecting restricted areas are **chain-**

153-846 O - 94 - 4 (Fold-in No. 1)

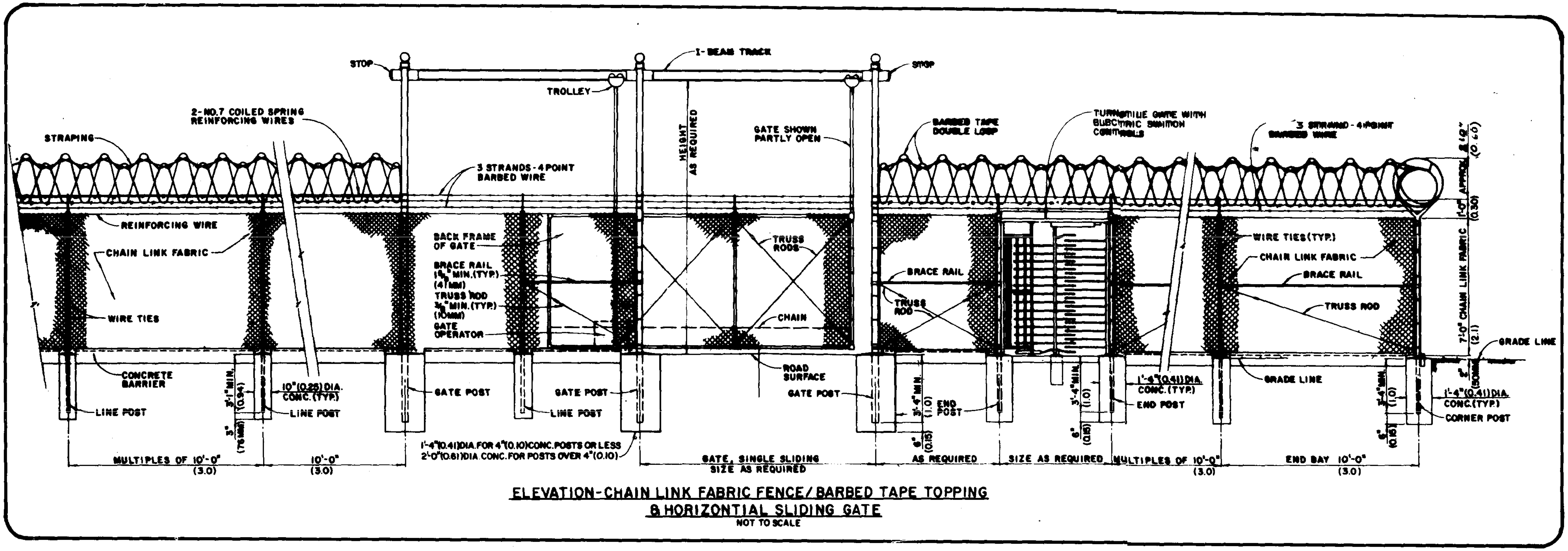


Figure 11—OCE drawing 40-16-10 of chain link fence construction.

link, barbed wire, concertina, and **barbed tape.** Choice of type depends primarily upon the degree of permanence of the installation, availability of materials, and time available for construction. Generally, chain-link fencing will be used for protection of permanent limited and exclusion areas. All four types of fencing maybe used to augment or increase the security of existing fences that protect restricted areas. Examples would be to create an additional barrier line, increase existing fence height, or provide other methods that add effectively to physical security.

a. Chain-link (Federal Spec. RR-F-191/1, Type I). Chain-link fence, including gates, must be constructed of 7-foot (approximately 2.13 m) material (6 foot or 1.83 m for controlled areas), excluding top guard. Fence heights for conventional arms/ammo security must be 6 feet for standard chain link, wire-mesh fencing. Chain-link fences must be of 9-gauge (.1508 inches or 3.77 mm) or heavier wire galvanized with mesh openings not larger than 2 inches (approximately 5.1 cm) per side, and a twisted and barbed selvage at top and bottom. It must be taut and securely fastened to rigid metal or reinforced concrete posts set in concrete. It must reach within 2 inches (5.1 cm) of hard ground or paving. On soft ground it must reach below the surface deeply enough to compensate for shifting soil or sand (OCE Guide Specification 02711). Security commensurate with FE-6 fence construction standards will be provided. Construction must be in accordance with specifications in Office, Chief of Engineers (OCE) drawing 40-16-10 (figure 11). For added resistance to climbing, optional top rail or taut wire may be omitted. Fencing may be painted with a nonreflective substance to reduce the glare to security forces (TM 5-830-3). Weaknesses in the chain link fence occur as a result of weather (rusting) and failure to keep fencing fastened to the post which affects the desired tightness.

b. Barbed Wire. Standard barbed wire is twisted, double-strand, 12-gauge wire, with four-point barbs spaced an equal distance apart. Barbed wire fencing, including gates, intended to prevent human trespassing should not be less than 7 feet (2.13 m) high,

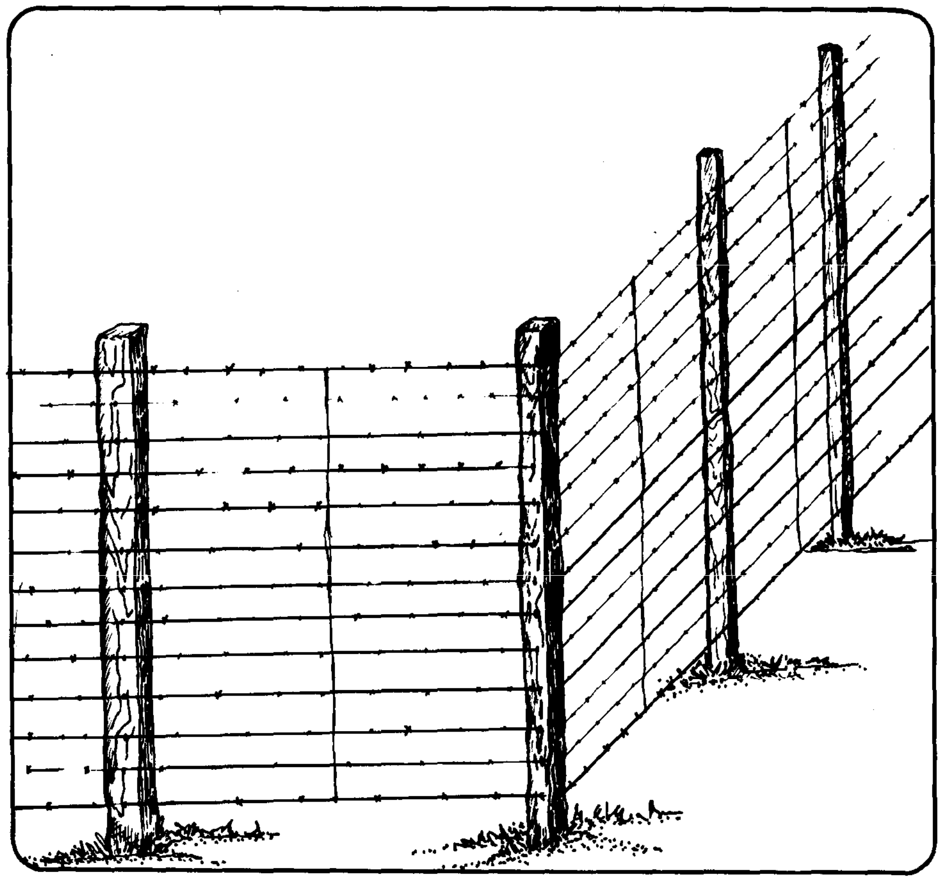


Figure 12—Example of properly constructed barbed wire fence.

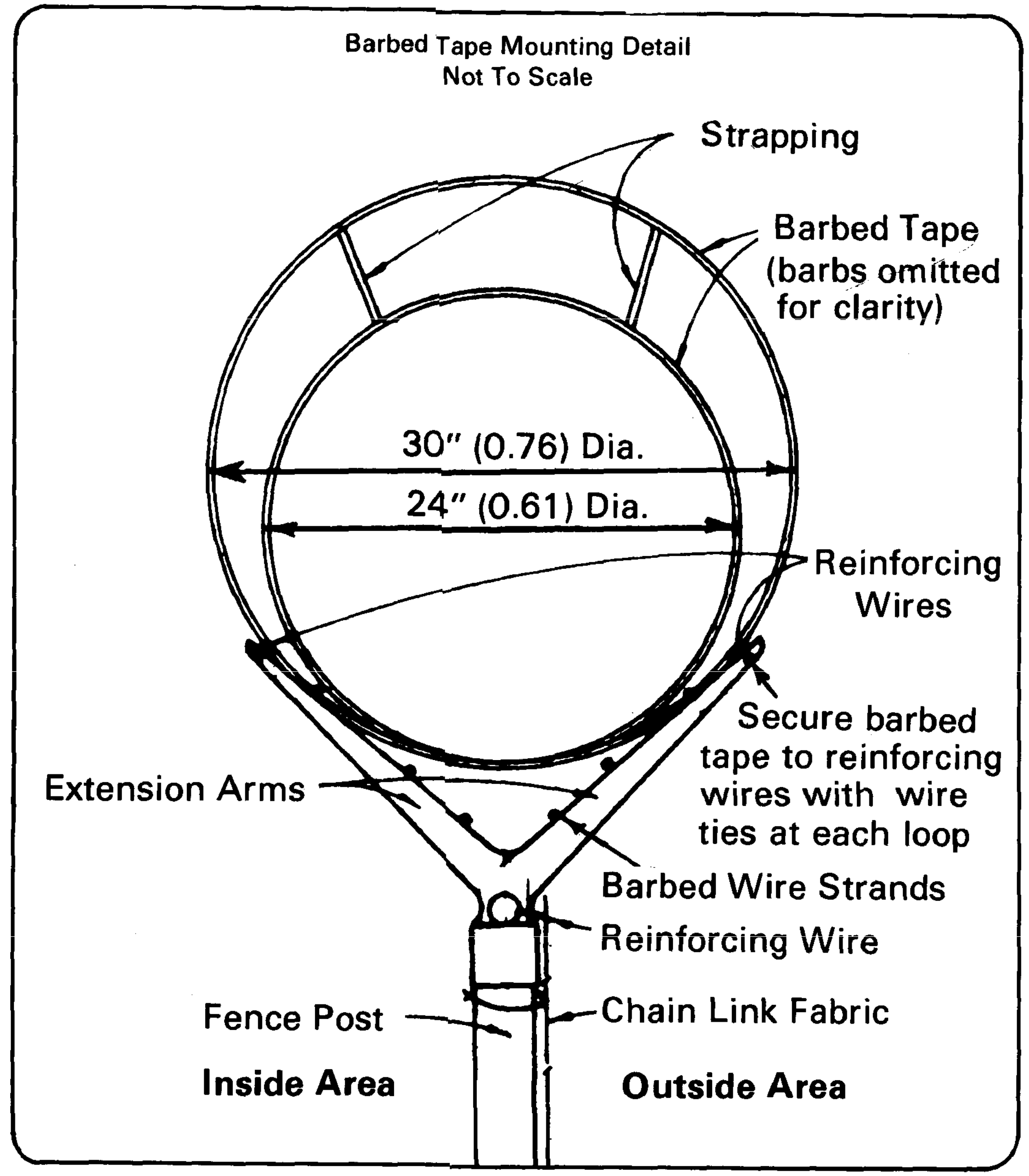


Figure 13—OCE drawing 40-16-10, barbed tape details.

excluding the top guard, and must be firmly affixed to posts not more than 6 feet (1.82 m) apart. The distance between strands will not exceed 6 inches (approximately 15.3 cm) and at least one wire will be interlaced vertically and midway between posts (figure 12).

c. Concertina. Standard concertina barbed wire is a commercially manufactured wire coil of high-strength-steel barbed wire, clipped together at intervals to form a cylinder. Opened, it is 50 feet long and 3 feet in diameter. When used as the perimeter barrier for a restricted area, concertina must be laid between poles with one roll on top of another or in a pyramid arrangement (minimum of three rolls). The ends must be staggered or fastened together and the base wire picketed to the ground.

d. Barbed Tape (Mil Fed Spec. MIL-B-52775A) (figure 13).

(1) The barbed tape system is composed of three items—barbed tape, barbed tape dispenser, and concertina tape. These items were type classified "standard A type," 16 December 1965.

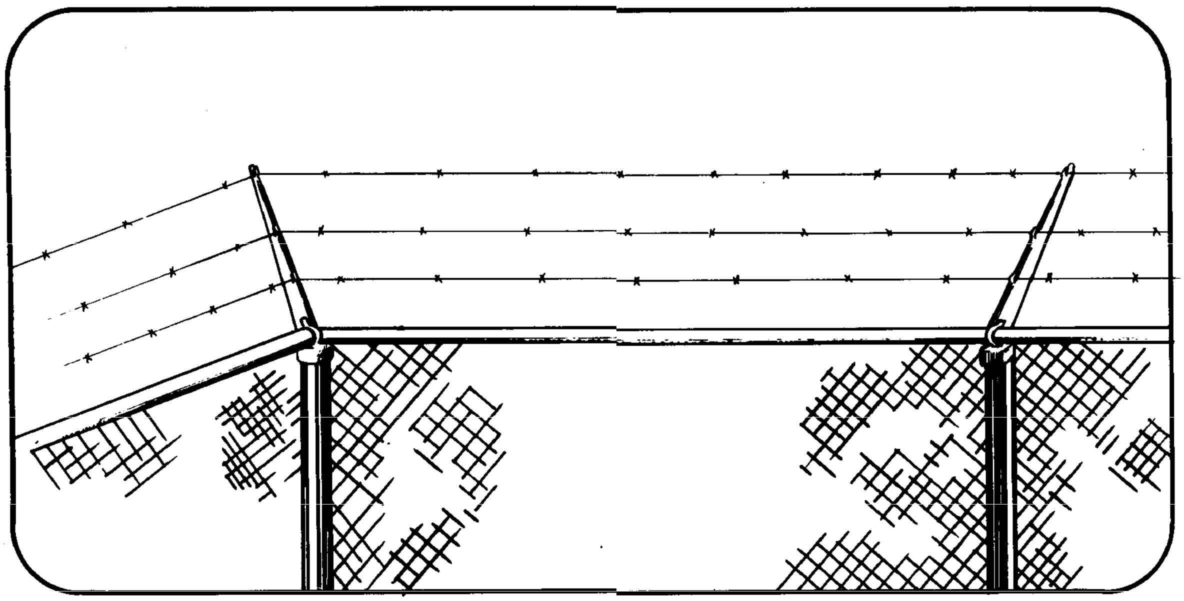


Figure 14—Supporting arms on top guard point outward.

(2) Barbed tape is fabricated from a steel strip (0.020 inches thick nominal) with a minimum breaking strength of 500 pounds. The overall width is 3/4 of an inch. The tape has 7/16-inch barbs spaced at 1/2 inch intervals along each side. Fifty meters of tape are wound on a plastic reel 8 3/4 inches in diameter and 1 inch thick. The finish is electro-galvanized 0.0001-inches thick on each side.

(3) Barbed tape concertina consists of a single strand of spring steel wire and a single strand of barbed tape. The sections between barbs of the barbed tape are securely clinched around the wire. Each coil is approximately 37 1/2 inches in diameter and consists of 55 spiral turns connected by steel clips to form a cylindrical diamond pattern when extended to a coil length of 50 feet. One end turn is fitted with four bundling wires for securing the coil when closed and each end turn is fitted with two steel carrying loops. The concertina extends to 50 feet without permanent distortion and when released, can be retracted into a closed coil.

(4) The handling of barbed tape requires the use of **heavy** barbed tape gauntlets (FSN 8415-926-1674) instead of standard barbed wire gauntlets.

e. Top Guard. A top guard must be constructed on all perimeter fences and may be added on interior enclosures for additional protection. A top guard is an overhang of barbed wire or barbed tape along the top of a fence, facing outward and upward at approximately a 45-degree angle (figure 14). Top guard supporting arms will be permanently affixed to the top of fence posts to increase the overall height of the fence at least 1 foot (approximately 30.5 cm). Three strands of barbed wire, spaced 6 inches (15.2 cm) apart, must be installed on the supporting arms. The number of strands of wire or tape may be increased when required. The top guard of fencing adjoining gates may range from a vertical height of 18 inches (45.7 cm) to the normal 45-degree outward protection, but only for sufficient distance along the fence to

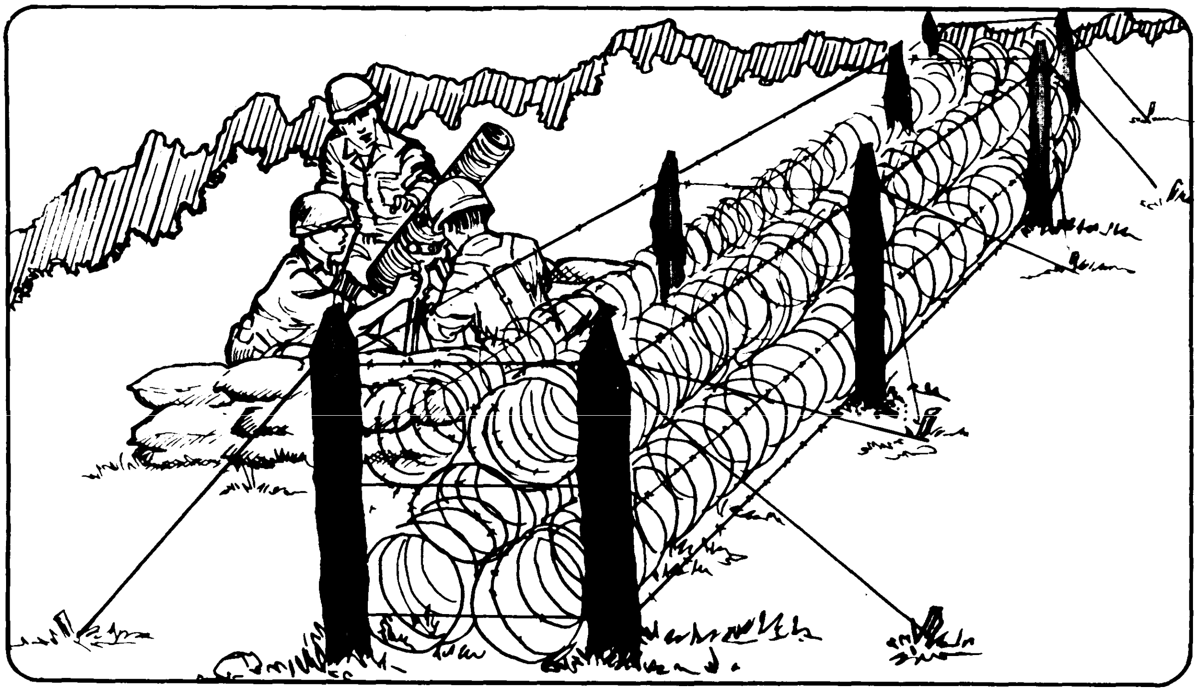


Figure 15—A type of field perimeter fence (cattle fence).

open the gate(s) adequately. Top fence rails should not be specified where protection is of utmost importance. Top rails will assist a climber. A bottom and top wire reinforcement should be used as a substitute (OCE-02711).

f. Gates and Entrances. The number of gates and perimeter entrances must be the minimum required for safe and efficient operation. Active perimeter entrances must be designed so that the guard force maintains full control. Semiactive entrances, such as infrequently used vehicular gates, must be locked on the inside when not in use. Gates and entrances, when closed, must provide a barrier structurally comparable to their associated barrier(s). Top guards, which may be vertical, are required for all gates.

g. Type Field Perimeter Fence. A combination of concertina fencing, developed in Vietnam, uses a double-barbed wire fence (the cattle fence described in FMs 5-15 and 100-50), with five rolls of concertina between the fences. This fence has, in many situations, been used in place of chain link fence, and has been found to be most effective (figure 15).

h. Tanglefoot Wire. Barbed wire or tape may be used in appropriate situations to construct a tanglefoot obstruction either outside a single perimeter fence or in the area between double fences, to provide an additional deterrent to intruders. The wire or tape should be supported on short metal or wood pickets spaced at irregular intervals of 3 to 10 feet, and at heights between 6 and 12 inches. The wire or tape should be crisscrossed to provide a more effective obstacle. Depth of the field is governed by the space and materials available.

5-5 Utility Openings

Sewers, air and water intakes and exhausts, and other utility openings of 10 inches (25.4 cm) or more in diameter that pass through perimeter barriers must have security equivalent to that of these barriers (TM 5-820-4).

a. Interior manhole covers 10 inches (25.4 cm) or more in diameter must be secured to prevent unauthorized opening.

b. Unavoidable drainage ditches, culverts, vents, ducts, and other openings having a cross-sectional area greater than 96 square inches (624 sq cm) and a smallest dimension greater than 6 inches (16.3 cm) will be protected by securely fastened welded bar grills (TM 5-280-4). As an alternative, drainage structures may be constructed of multiple pipes, each pipe having a diameter of 10 inches (25.4 cm) or less. Multiple pipes of this diameter also may be placed and secured in the inflow end of a drainage culvert to prevent intrusion into the area. (See examples in figure 16.)

5-6 Other Perimeter Barriers

a. Building walls and roofs, when serving as perimeter barriers, must be constructed and arranged to provide uniform protection equivalent to that provided by chain-link fencing. If a building less than two stories high forms part of the perimeter, a top guard must be used along the outside coping to deny access to the roof (figure 17).

b. Masonry walls, when used as perimeter barriers, must have a minimum height of 7 feet (approximately 2.13 m) and must have a barbed wire top guard, sloped outward at a 45-degree angle, carrying at least three strands of barbed wire and increasing the vertical

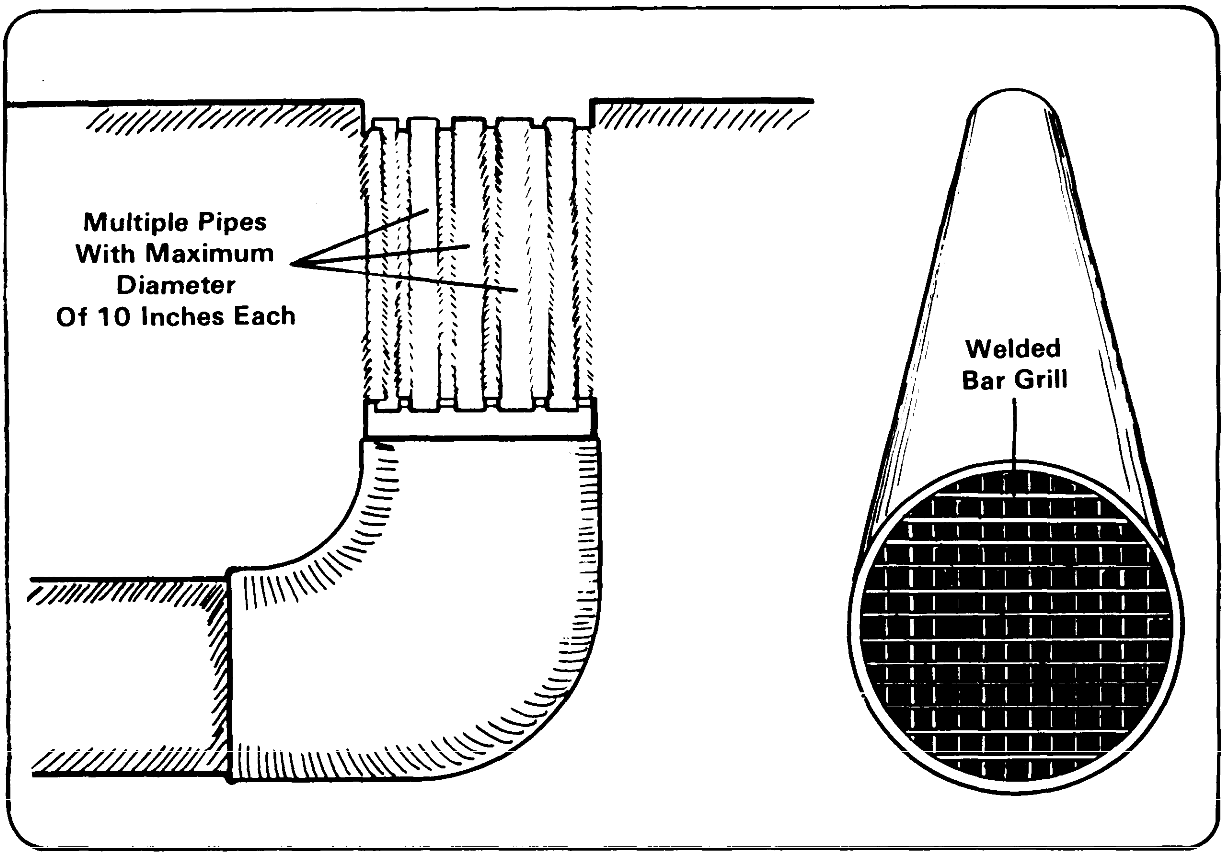


Figure 16—Examples of secured utility openings.

height of the barrier by at least 1 foot (approximately 30.5 cm); or they must have a minimum height of 8 feet (2.4 m) and have broken glass, set on edge and cemented to the top surface.

c. Windows, active doors, and other designated openings must be protected by securely fastened bars, grills, or chain-link screens. Window barriers must be fastened from the inside If hinged, the hinges and locks must be on the inside. If an instrusion detection system is used, consideration should be given to using the security screen detailed in OCE drawing DEF 40-26-01.

d. Construction Procedures. Detailed guidance on construction procedures, material and manpower requirements for field construction of barriers by small troops units is in FM 5-15.

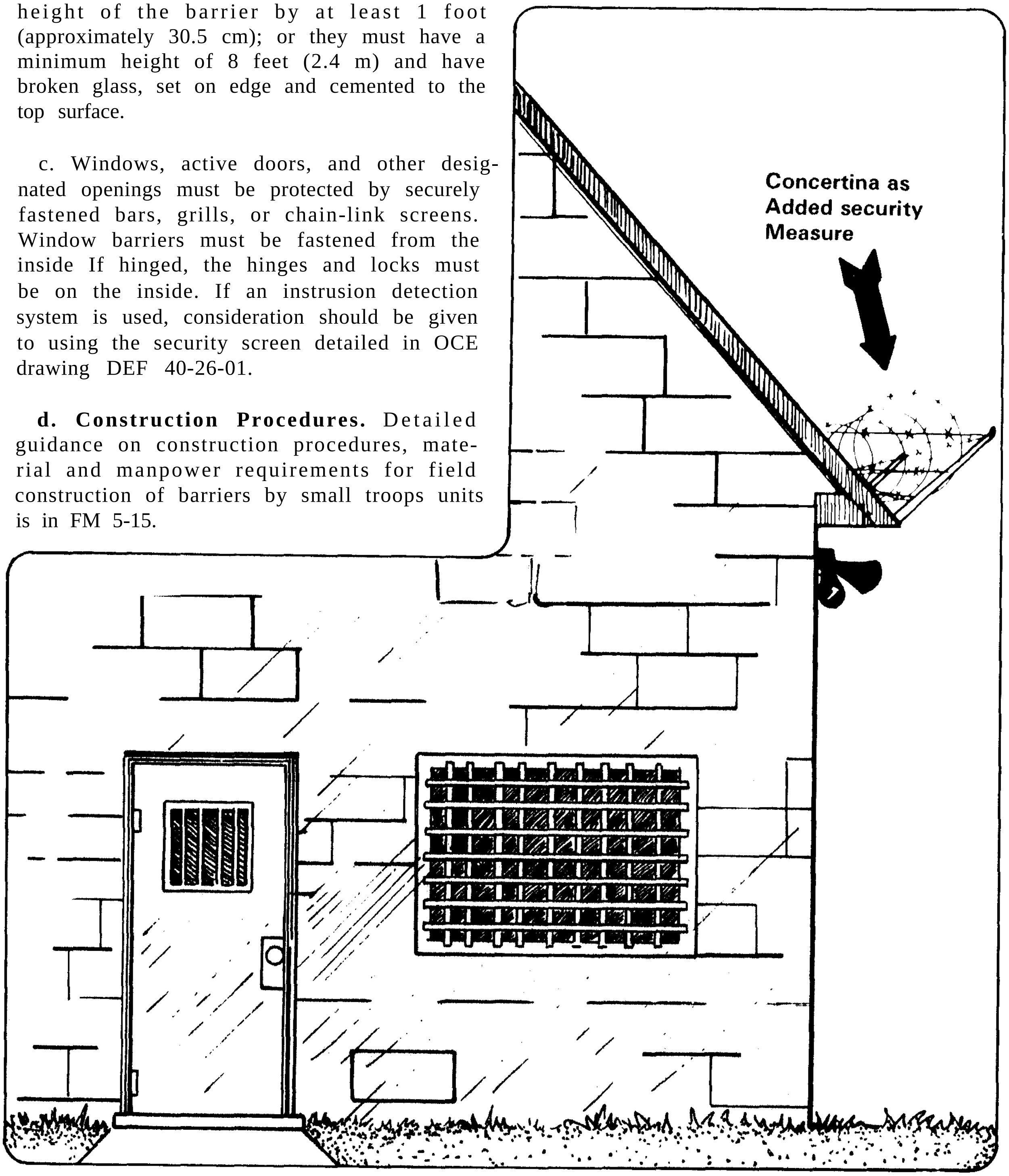


Figure 17 - Sample of top guard on roof.

153-846 0 - 94 - 6

5-7 Security Tower Design

Reliance on towers as the only means for observation of a perimeter is usually considered unsatisfactory. However, all towers should be located to provide maximum observation and be constructed for protection from small arms fire.

a. Mobile towers are useful in some temporary situations, such as a large open storage area where there is activity in receiving and storing equipment. All facilities that use towers must have a support force available for emergencies, and tower personnel should be rotated at frequent intervals.

b. Psychologically, the mere elevation of the observer has an unnerving effect on a potential intruder. However, as mentioned above, the isolation of the tower tends to reduce the alertness of its occupants.

c. The **height of a tower** increases the range of observation during daylight hours and at night with artificial illumination. However, during inclement weather and during blackout, towers lose this advantage and must be supplemented by on-the-ground observation.

5-8 Tower Use

In **planning the use of towers,** consideration must be given to the following:

a. A possible necessity for hardening the tower (by use of sandbags, salvage armor-plating, etc.) to protect the occupant. This may require strengthening of the support, which should be performed only under the supervision of an engineer.

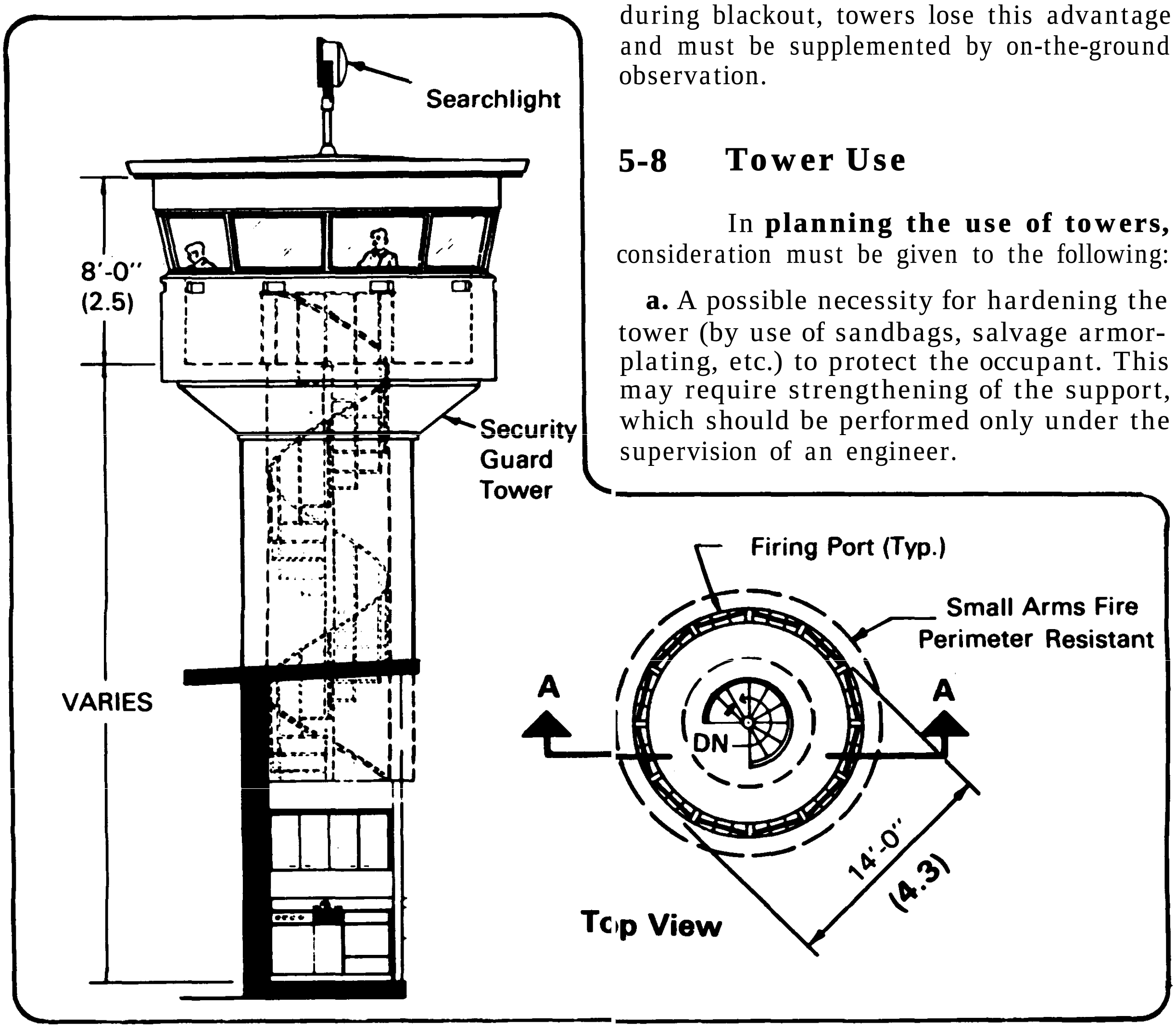


Figure 18—Details of tower design.

b. Communications and alarm systems, both audible and visual (primary and alternate).

c. The possibility of using appropriate STANO equipment with the tower and perimeter barriers being surveilled. Some of the infrared items may be especially valuable.

d. Protective lighting (chapter 6, AR 50-5).

e. Protection of the route to the tower.

f. Height of the tower according to the area of observation.

g. Mutually supporting in terms of small arms fire.

h. Allows for egress and ingress of supporting alert forces, as appropriate.

i. Backed up by a fortified defensive fighting position, as appropriate.

j. Located within the exclusion area. (See figure 18 for tower design details.)

5-9 Installation/Activity Entrances

a. The number of installation/activity gates and perimeter entrances inactive use should be limited to the minimum required for safe and efficient operation of the installation. Protective lighting must be IAW chapter 6 of this manual. When necessary, crash beams should be installed in front of vehicle gates according to the design specifications in figure 19.

b. Entrance plans (primary and alternate) for an installation or activity to control vehicle traffic using guard personnel is outlined in figures 20 and 21 on page 76. The type guard post used to support the entrance plans is detailed in figure 22.

c. Active perimeter entrances should be designated so security forces maintain full control without unnecessary delay in traffic. This is largely a matter of having sufficient entrances to accommodate the peak flow of

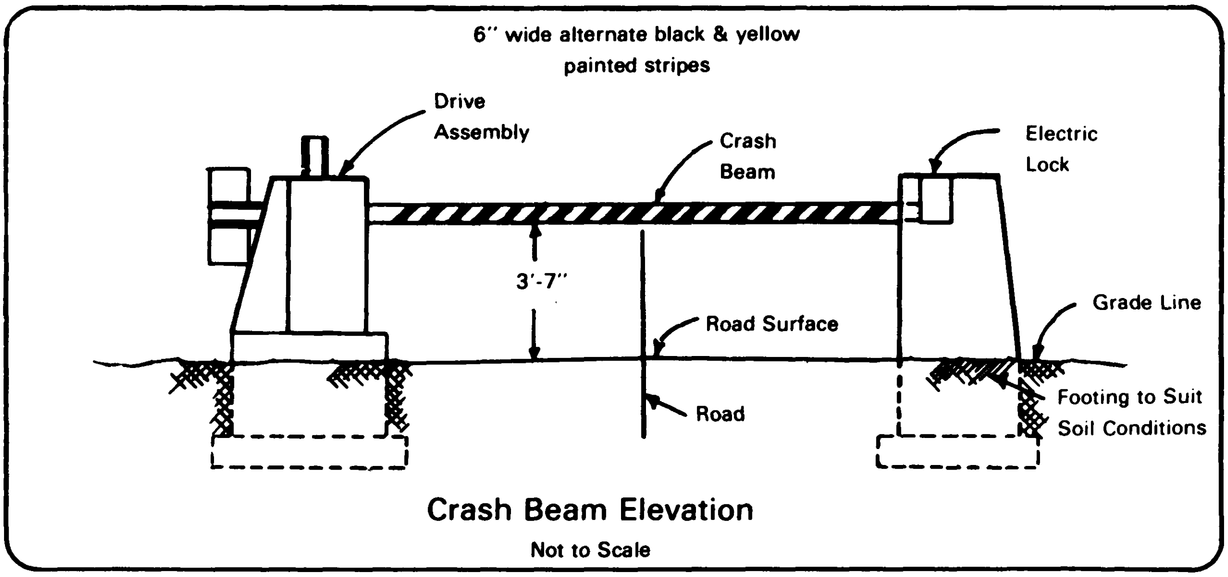


Figure 19—OCE drawing 40-16-10 crash beam details.

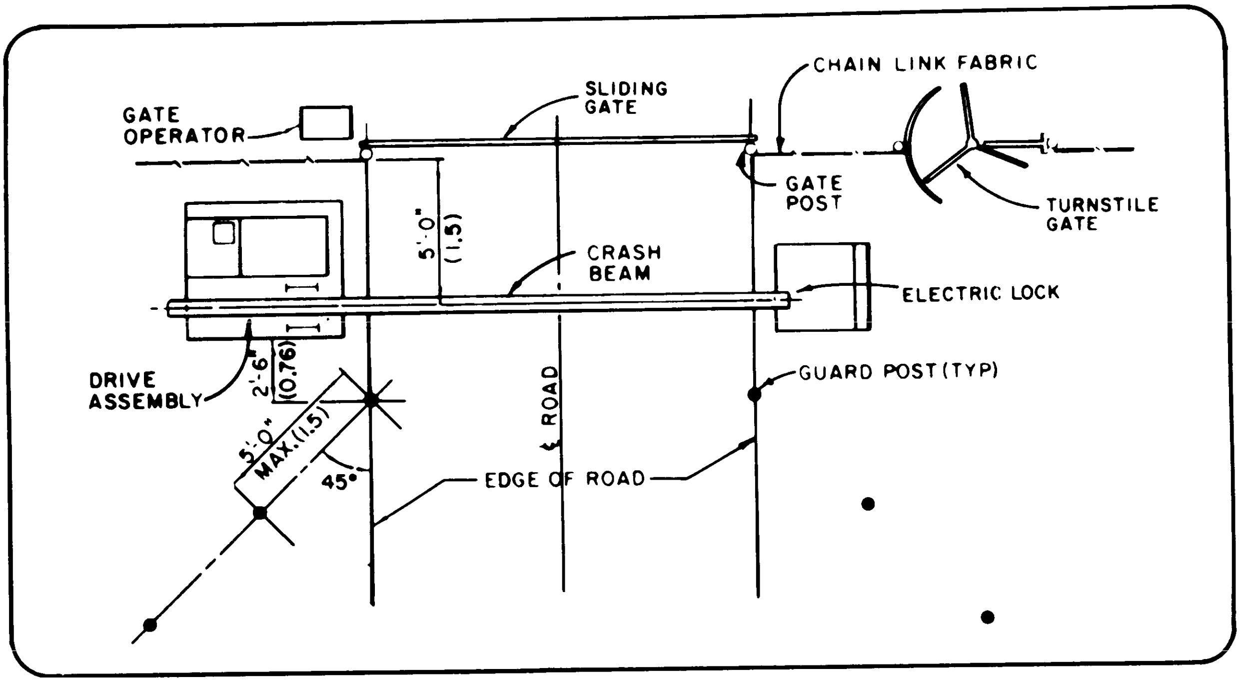


Figure 20—Primary entrance plan.

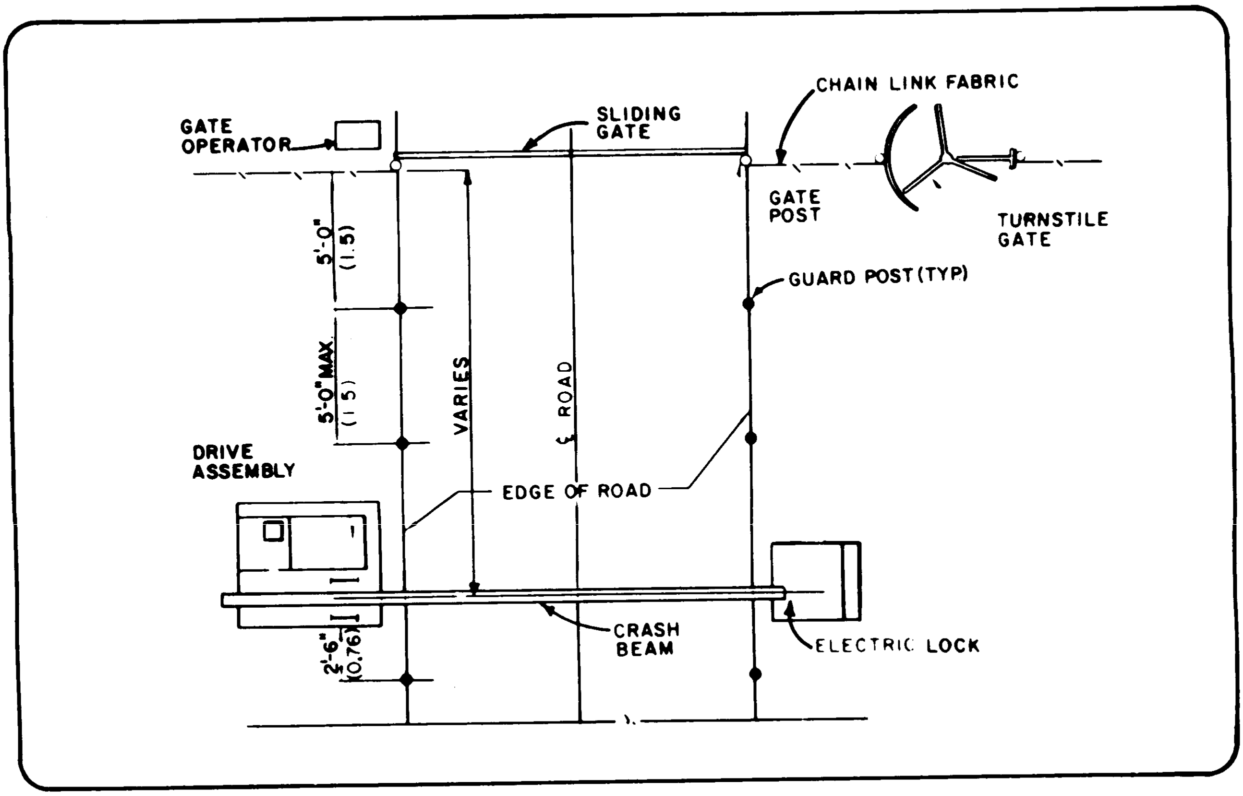


Figure 27—Alternate entrance plan.

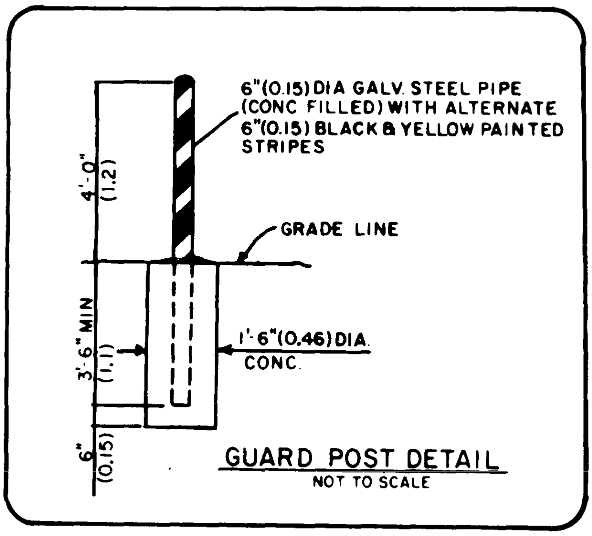


Figure 22—Guard post support plan.

pedestrian and vehicular traffic, and adequate lighting for rapid and efficient inspection. When gates are not manned during nonduty hours, they should be securely locked, illuminated during hours of darkness, and periodically inspected by a roving patrol. This also applies to doors and windows that form a part of the perimeter.

d. Semiactive entrances, such as extra gates for use during peak traffic flow and railroad siding gates, should be locked at all times when not guarded. Keys to such entrances should be in the custody of the provost marshal (security manager) or the chief of the security force, and should be strictly controlled (chapter 8).

e. Inactive entrances (those used only occasionally) should be kept locked and be subject to the same key control and inspection as semiactive entrances.

f. Sidewalk elevators and any other utility openings that provide access to areas within the perimeter barrier should be locked, guarded, or otherwise provided security equivalent to that of the perimeter barrier.

5-10 Entry Control Stations

Entry control stations normally should be provided at main perimeter entrances where such entrances are manned by security personnel on a full-or part-time basis. Considerations for construction and use should be based, in part, on the information outlined in paragraphs 5-8 and 5-9.

a. Entry control stations should be located as near as practicable to the perimeter entrance to permit personnel inside the station to maintain constant surveillance over the entrance and its approaches.

b. Entry control stations that are manned 24 hours each day should have interior and exterior lighting, interior heating (where appropriate) and sufficient glassed area to afford adequate observation for personnel inside. Where appropriate, entry control stations should be designed for optimum personnel identification and movement control (chapter 4).

c. Equipment in a station should include:

(1) Telephone or radio.

(2) Badge racks.

(3) Electronic boards for checking lights.

d. Procedures for hardening against attack.

(1) Reinforced concrete.

(2) Steelplating and bullet-proof glass.

(3) Sandbags two layers in depth.

5-11 Signs and Notices

Signs should be plainly displayed and be legible from any approach to the perimeter from a reasonable distance. The size and coloring of such signs, lettering thereon, and the interval of posting must be appropriate to each situation.

a. Control Signs. Signs should be erected where necessary to assist in control of authorized entry, to deter unauthorized entry, and to preclude accidental entry.

b. Warning Signs.

(1) A system must be provided to warn intruders that the arena is restricted and that trespassing may cause the use of deadly force. The system must include warning signs and a method of challenging intruders.

(2) Warning signs must be installed along the limited area physical barriers and at each entry point so they can be seen readily and understood by anyone approaching the perimeter. In areas where English is but one of two or more languages commonly spoken, warning signs must contain the local language(s), in addition to English; and the wording on the signs will denote warning of a restricted area. Warnning signs must be positioned on or outside the limited area physical barrier and should be at intervals of no more than 100 feet (30.5 m).

(3) Signs must not be mounted on fences equipped with IDA equipment because nuisance alarms could be caused by environmental movement of the signs. Additionally, the restricted area warning signs prescribed in AR 380-20 must be posted at all entrances to limited and exclusion areas.

c. Other Signs.

(1) Signs setting forth the **conditions of entry** to an installation or area should be plainly posted at all principal entrances and should be legible under normal conditions at a distance not less than 50 feet from the point of entry. Such signs should inform the entrant of the provisions of search of the person, vehicle, packages, etc., or prohibitions (such as against cameras, matches, lighters, entry for reasons other than official business, etc.) that may be prescribed by the installation commander (AR 210-10).

(2) Signs or notices legibly setting forth the designation of **restricted areas** and provisions of entry thereto should be plainly posted at all entrances and at other points along the perimeter line as necessary. The wording of such signs or notices is prescribed in AR 380-20, and chapter 4; section III of this manual.

5-12 Installation/Activity Perimeter Roads And Clear Zones

When the perimeter barrier encloses a large area, an interior all-weather perimeter road should be provided for security patrol vehicles. Clear zones should be maintained on both sides of the perimeter barrier to provide an unobstructed view of the barrier and the ground adjacent to it.

a. Roads should meet these requirements:

(1) Be within the clear zone and as close to the perimeter barrier as possible, but not close enough to cause soil erosion.

(2) Constructed to allow for effective road barriers to deter motor movement of unauthorized personnel during mobilization periods.

b. Clear Zones.

(1) Clear zones should be kept clear of weeds, rubbish, or other material capable of offering concealment or assistance to an intruder attempting to breach the barrier.

(2) A clear zone of 20 feet or more should exist between the perimeter barrier and exterior structures, parking areas, and natural or manmade features. When possible, a clear zone of 50 feet or more should exist between the perimeter barrier and structures within the protected area, except when a building wall constitutes part of the perimeter barrier.

(3) When it is impossible to have adequate clear zones because of property lines or natural or manmade features, an increase in the height of the perimeter barrier, increased security patrol coverage, more protective lighting, or an intrusion detection device along that portion of the perimeter barrier may be necessary.

5-13 Protection In Depth

a. On a very large installation such as a proving ground, it is obviously impracticable to construct an expensive perimeter fence and to keep it under constant observation. Such an installation is usually estab lished in a sparsely inhabited area. Its comparative isolation and the depth of the installation itself give reasonable perimeter protection. Under these circumstances the posting of warning signs or notices, reducing access roads to a minimum, and periodic patrols in the area between the outer perimeter and the conventionally protected vital area of the installation may be sufficient.

b. An alternate to erecting new or replacing old chain-link fence involving an entire installation, perimeter is to relocate/isolate the sensitive area or item by:

(1) Relocating the item within a safe perimeter.

(2) Consolidating the item with other items.

(3) Erecting a chain-link fence (regulation permitting).

5-14 Nuclear Weapons Construction Design Criteria

For design and construction criteria, see DOD Directive 5210.41M and AR 50-5.

The interest of security must be kept in mind when walls, ceilings, floors, and roofs are constructed. Facilities that house arms and ammunition should be constructed as security barriers in the interest of deterring penetration. Protection should be equivalent to that provided by chain-link fencing.

Arms Facility Structural Standards — Section II

5-15 Wall Construction Standards

a. Walls should consist of 8 inches of concrete reinforced with No. 4 bars on 9-inch centers in each direction and staggered on each face to form a grid approximately 4 ½ inches square. An alternative 8-inch concrete block with No. 4 bars threaded through block cavities at 8-inch centers, with the cavities then filled with mortar or concrete and with horizontal joints reinforced at every course. As a minimum alternative, use 8 inches of brick interlocked between inner and outer courses. These options are stated in order of most to least secure.

b. Selection must depend on local threat and vulnerability.

c. See AR 190-11 for information concerning USAR consolidated arms storage facilities.

5-16 Ceiling Construction Standards

a. The ceiling of the arms storage facility must be reinforced concrete, structurally designed for the spans between supporting walls. The resulting slab should offer security comparable to that provided by the walls.

b. If the ceiling is of concrete pan joist construction, the pans must be reduced in depth over the vault area so the thinnest portion is not less than 6 inches and the clear space between joists does not exceed 20 inches. The reinforcing grid requirement for flat slab construction also applies.

c. Reinforcing bar spacing should form a grid in which the area of any opening does not exceed 96 square inches, using No. 4 bars or larger.

5-17 Floor Construction Standards

Floor slab thickness, if on grade, should be a minimum of 6 inches reinforced with 6x6—W4xW4 mesh or equivalent bars. If the floor forms the ceiling of an underlying room or area, the ceiling standards apply.

5-18 Windows and Entrances

a. Entrances and issue windows should have two doors.

b. Doors should be 1 3/4 inch-thick, solid wood doors with 12-gauge metal plate securely attached to the outside face; or standard 1 3/4-inch-thick, hollow metal, industrial type doors (minimum thickness of skin plate 14-gauge) internally reinforced vertically with continuous steel stiffeners spaced 6 inches maximum on center.

c. The locking device used on the most secure door (usually the inner door) must be a high security padlock and hasp (MILP-43607). The other door must have a secondary padlock (MILP-17802B) or an equivalent mortise cylinder lock approved by the Intelligence Material Development Officer, Ft. Holabird, Maryland.

d. One of the doors in the double-door concept may be a rod and bar grid door; and the other may be either solid wood with metal plate or hollow metal. Grid doors must be constructed of 1 1/4-inch x 3/8-inch flat steel bars horizontal at 8 inches maximum on center, and l/2-inch diameter rods vertical at 4 inches maximum on center welded to, or passing through, the 1 l/4-inch surface of the flat bars, resulting in a grid with openings of 32 square inches or less.

e. The grid door is more suitable for accommodating the high security hasp (MIL P-43607D) and should be used as the inner door. Door hinges must be fixed-pin security type, safety-stud hinges, or must have hinge pins spot-welded to prevent removal. Hinge mounting screws will not be exposed to the outside of the arms room.

f. Frames must be compatible with adjacent doors and walls and must be securely anchored.

g. Class 5 steel vault door (Fed. Spec. AA-D-600B) with a built-in three-position, dial-type, changeable combination lock may be used in lieu of the two doors described above. A vault door day-gate does not provide adequate penetration resistance for an unattended vault, and, if used, should be intended only to prevent inadvertent entry when the vault is open and occupied.

(1) Anchor rings in arms and ammunition vault construction should be placed every 6 feet along the length of each wall.

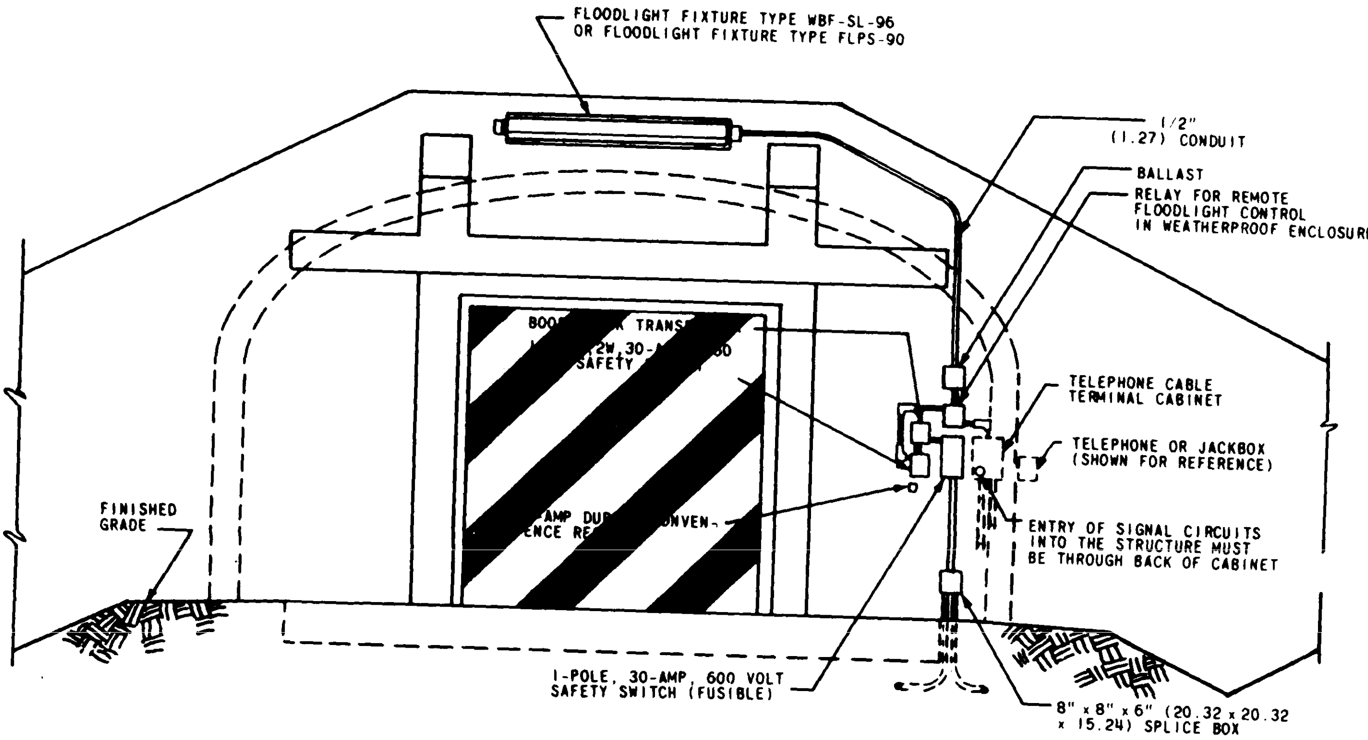
(2) Review Engineer Technical Letter, 1110-3-229, 11 Apr 75, and definitive drawing, DEF 33-33-18, Consolidated Storage Building.

h. Openings such as windows should be limited to meet the essential minimum, or be eliminated entirely by removal and sealing of the resultant openings with material comparable to that forming the adjacent walls. Any required windows or openings greater than 96 square inches (the smallest dimension is greater than 6 inches) must be protected by a rod-and-bar grid as described in AR 190-11. Grid ends should be imbedded in the structure or welded to a frame that is securely attached to the structure from the inside.

NOTE: It is next to impossible to build a protective barrier that cannot be penetrated by a human or heavy armor. Therefore, as opposed to protecting an installation or facility using only one barrier, a combination of barriers will provide security as discussed in chapter 2.

Chapter 6

Protective Lighting



Protective lighting provides ameans of continuing, during hours of darkness, a degree of protection approaching that maintained during daylight hours. This safeguard also has considerable value as a deterrent to thieves and vandals and may makethe job of the saboteur more difficult. It is an essential element of an integrated physical security program.

6-1 Requirements

a. Protective or security lighting needs at installations and facilities depend upon each situation and the areas to be protected. Each situation requires careful study to provide the best visibility practicable for such security duties as identification of badges and people at gates (chapters 4 and 5), inspection of vehicles, prevention of illegal entry, detection of intruders outside and inside buildings and other structures, and inspection of unusual or suspicious circumstances.

b. When such lighting provisions are impractical, additional security posts, patrols, sentry dog patrols, or other security means will be necessary.

c. Protective lighting should not be used as a psychological deterrent only. It should be used on a perimeter fence line only where the fence is under continuous or periodic observation. Protective lighting may be unnecessary where the perimeter fence is protected by a central alarm system.

d. Protective lighting maybe desirable for those sensitive areas or structures within the perimeter, which are under specific observation. Such areas or structures include pier and dock areas, vital buildings, storage areas, and vulnerable control points in communications, power, and water distribution systems. In interior areas where night operations are conducted, adequate lighting of the area facilitates detection of unauthorized persons approaching or attempting malicious acts within the area.

6-2 Characteristics

fighting is inexpensive to maintain and, when properly employed, may reduce the need for security forces. It may also provide personal protection for forces by reducing the advantages of concealment and surprise for a determined intruder. security forces thus relieved may be used to better advantage elsewhere.

Protective lighting usually requires less intensity than working light, except for identification and inspection at authorized portals and in emergencies. Each area of an installation or facility presents its particular problem based on physical layout, terrain, atmospheric and climatic conditions, and the protective requirements. Data are available from the manufacturers of lighting equip ment and from the Army Corps of Engineers, which will assist in designing a lighting system. Included in these data are:

- Descriptions, characteristics, and specification of various incandescent, arc, and gaseous discharge lamps.
- Lighting patterns of the various luminaries.
- Typical layouts showing the most efficient height and spacing of equipment.
- Minimum protective lighting intensities required for various applications.

6-3 Commander's Responsibility

a. Each commander must determine perimeter lighting needs dependent upon the threat, perimeter extremities, surveillance capabilities, and the available guard forces.

b. He must insure that protective lighting is designed and employed to discourage unauthorized entry and to facilitate detection of intruders approaching or attempting to gain entry into protected areas.

c. The commander must insure that protective lighting operates continuously during periods of reduced visibility, and that standby lighting is maintained and periodically tested for use during times of emergency and mobilization alerts.

6-4 Planning Considerations

In planning a protective lighting system, the physical security manager must give specific consideration to the following areas:

a. Cleaning and replacement of lamps and luminaries, particularly with respect to costs and means (such as ladders, mechanical buckets, etc.) required and available.

b. Advisability of including **mercury and photoelectric controls.** These may be desirable in a peacetime situation, but undesirable when blackout is a possibility.

c. The effects of local **weather conditions** on various types of lamps and luminaries.

d. Fluctuating or **erratic voltages** in the primary power source.

e. Requirement for **grounding of fixtures** and the use of a common ground on an entire line to provide a stable ground potential.

f. Establishment of a ledger to maintain a **burning-time (80 percent)** record based on the life expectancy of the lamp. The ledger should contain as a minimum the following:

- Type and wattage of lamp.
- Area, facility, or utility pole used.
- Date of insertion.
- Programed date (based on life expectancy) for extraction and where used (admin area).

g. Limited and exclusion areas.

(1) All limited and exclusion areas must have protective lighting on a permanent basis at perimeter and access control points. The lighting must be positioned to:

(a) Prevent glare that may temporarily blind the guards.

(b) Avoid silhouetting or highlighting the guards.

(2) Lighting in these areas must be under the control of the security force.

(3) The perimeter band of lighting must provide a minimum intensity of 0.2 foot candles, measured horizontally 6 inches (15.2 cm) above ground level, at least 30 feet (9.1 m) outside the exclusion area barrier. Lighting inside exclusion areas or on structures containing nuclear weapons must be of sufficient intensity to enable detection of persons in the area or at structure entrance(s). fighting at entrance control points must be of sufficient intensity to enable guards to compare and identify bearers and badges.

(4) Protective lighting systems will be operated continuously during hours of darkness.

(5) Protective lights should be employed so that the failure of one or more lights will not affect the operation of remaining lights.

h. Interior and exterior arms storage lighting. Interior and exterior security lighting must be provided as follows for all arms storage facilities, buildings in which arms storage rooms are located, arms storage rooms, motor pools, hangars, and outdoor parking areas for vehicles or aircraft that have weapons stored on board:

(1) During hours of darkness, exterior entrances of arms buildings and motor pool bays and hangars where vehicles or aircraft are parked with weapons aboard must be illuminated to an intensity of not less than 1.0 foot candle at any point to a height of 8 feet on their vertical surfaces and to a horizontal distance of 8 feet from the entrance.

(2) Interior entrances of arms rooms must be illuminated a minimum of 0.10 foot candle at any point within a 20-foot radius of the entrance.

(3) Vehicles and aircraft parked outside with weapons aboard must be illuminated 0.10 foot candle at any point within a 30-foot radius of the vehicle or aircraft.

(4) Switches for exterior lights must be installed so they are not accessible to unauthorized individuals. Exterior lights must be covered with wire mesh screen or other material that will prevent their being broken by thrown objects.

(5) New construction lighting requirements must conform to ammunition and explosive safety requirements of appendix C, TM 9-1300-206.

(6) Lighting requirements on existing facilities should be programed for and upgraded as needed.

i. Other Suitable Employment Locations:

(1) Warehouses

(2) Motorpools/parks

(3) Commissaries

(4) Post exchanges/annexes

(5) Clubs (EM, NCO, Officer, Country)

(6) Bank/finance and accounting office

(7) Medical/dental facilities

(8) Salvage yards

(9) Helipads and hangars

(10) Museums

(11) Gasoline dispensing areas

(12) Recreational areas (isolated/administrative areas)

(13) Troop billet areas

(14) Individual troop movement areas

(15) Housing areas

(16) Perimeter entrances/exits (isolated/used)

(17) Troop working areas.

6-5 Principles Of Protective Lighting

Protective lighting should enable guard force personnel to observe activities around or inside an installation without disclosing their presence. Adequate lighting for all approaches to an installation not only discourages attempted unauthorized entry, but also reveals persons within the area. However, lighting should not be used alone. It should be used with other measures such as fixed security posts or patrols, fences, and alarms. Other principles of protective lighting are listed next.

a. Good protective lighting is achieved by adequate, even light upon bordering areas, glaring lights in the eyes of the intruder, and relatively little light on security patrol routes. In addition to seeing long distances, security forces must be able to see low contrasts, such as indistinct outlines of silhouettes, and must be able to spot an intruder who may be exposed to view for only a few seconds. All of these abilities are improved by higher levels of brightness.

b. In planning protective lighting, high brightness contrast between intruder and background should be the first consideration. With predominantly dark dirty surfaces or camouflage type painted surfaces, more light is needed to produce the same brightness around installations and buildings than when clean concrete, light brick, and grass predominate. When the same amount of light falls on an object and its background, the observer must depend on contrasts in the amount of light reflected. The ability of the observer to distinguish poor contrasts is significantly improved by increasing the level of illumination.

c. When the intruder is darker than his background, the observer sees primarily the outline or silhouette. Intruders who depend on dark clothing and even darkened face and hands may be foiled by using light finishes on the lower parts of buildings and structures. Stripes on walls have also been used effectively, as they provide recognizable breaks in outlines or silhouettes. Good observation conditions can also be created by providing broad lighted areas around and within the installation, against which intruders can be seen.

d. Two basic systems, or a combination of both may be used to provide practical and effective protective lighting. The first method is to light the boundaries and approaches. The second is to light the area and structures within the general boundaries of the property.

e. To be effective, protective lighting should:

(1) Discourage or deter attempts at entry by intruders. Proper illumination may lead a potential intruder to believe detection is inevitable.

(2) Make detection likely if entry is attempted.

6-6 Types of Lighting

The type of lighting system to be used depends on the overall security requirements of the installation concerned. Lighting units of four general types are used for protective lighting systems-continuous, standby, movable, and emergency.

a. Continuous lighting (stationary luminary). This is the most common protective lighting system. It consists of a series of fixed luminaries arranged to flood a given area continuously during the hours of darkness with overlapping cones of light. Two primary methods of employing continuous lighting are glare projection and controlled lighting:

(1) The glare projection lighting method is useful where the glare of lights directed across surrounding territory will not be annoying nor interfere with adjacent operations. It is a strong deterrent to a potential intruder because it makes it difficult for him to see the inside of the area. It also protects the guard by keeping him in comparative darkness and enabling him to observe intruders at considerable distance beyond the perimeter. (See figure 23 for installation details.)

(a) Glare projection or other protective perimeter lighting may not be appropriate in some instances. In combat, tactical perimeter security considerations are given first priority over security against pilferage. Generally, the tightening of tactical perimeter security strengthens other physical security efforts. A blending of tactical and physical security principles is required—especially true with regards to perimeter lighting.

(b) Glare projection is not appropriate where security troop emplacements may be silhouetted or illuminated for the enemy to see from the enemy's approach to the secured site. Where glare projection is desired, security troops placed in front of the perimeter fence should be moved, but still be able to take up effective fields of fire for defense of the perimeter. If such blending of protective lighting and tactical security cannot be accomplished, perimeter lighting should not be used. Floodlights that provide a band of light with great horizontal angular dispersal and which directs the glare at a possible intruder while restricting the downward beam, is preferred in this application.

(2) Controlled lighting is best when it's necessary to limit the width of the lighted strip outside the perimeter because of adjoining property or nearby highways,

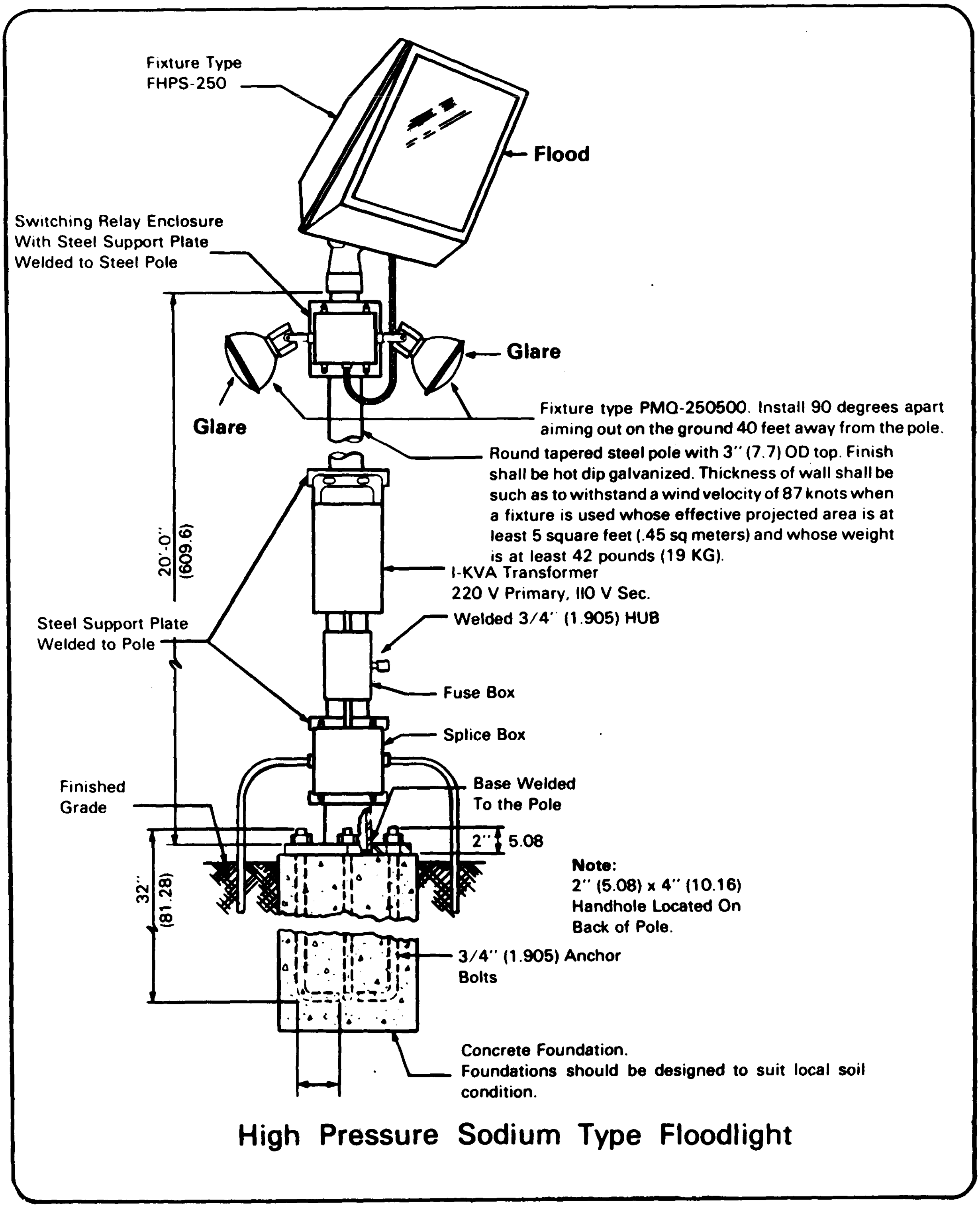


Figure 23—Typical perimeter security lighting details.

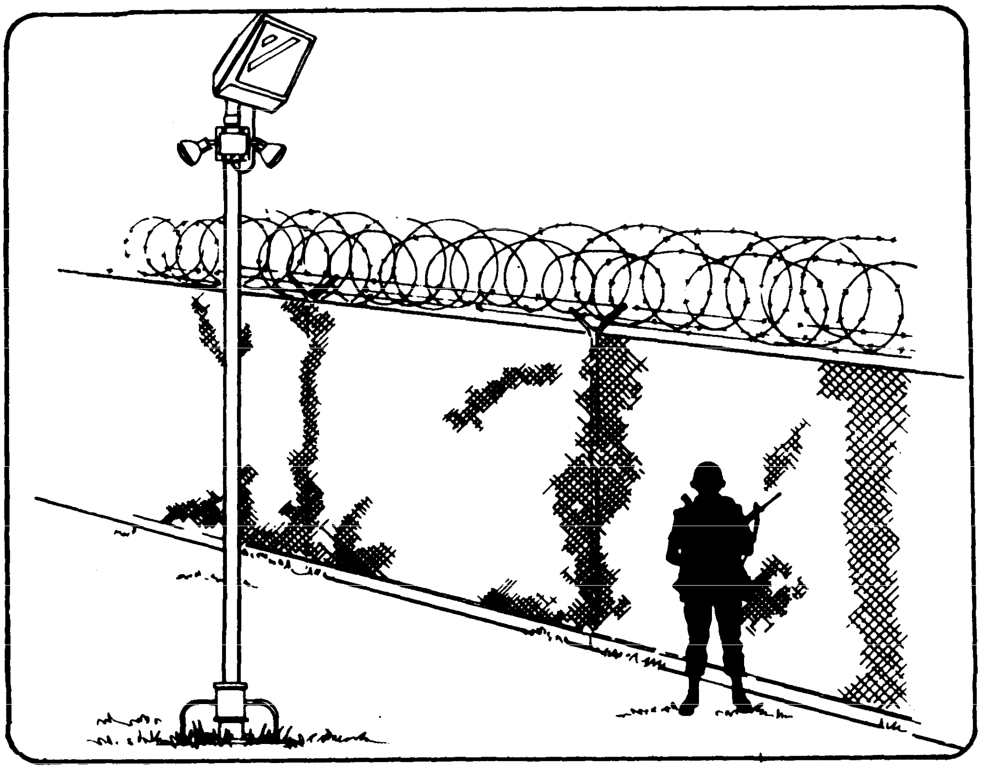


Figure 24—Example of boundary lighting near adjoining property (controlled lighting).

railroads, navigable waters, or airports. In controlled lighting, the width of the lighted strip can be controlled and adjusted to fit the particular need, such as illumination of a wide strip inside a fence and a narrow strip outside; or floodlighting a wall or roof. This method of lighting often illuminates or silhouettes security personnel as they patrol their routes (figure 24 shows controlled lighting).

b. Standby lighting (stationary luminary). The layout of this system is similar to continuous lighting. However, the luminaries are not continuously lighted, but are either automatically or manually turned on only when suspicious activity is detected or suspected by the security force or alarm systems.

c. Movable lighting (stationary or portable). This type of system consists of manually operated movable searchlights which may be either lighted during hours of darkness or lighted only as needed. The system normally is used to supplement continuous or standby lighting. (The 18-inch 2.2 KW Xeon searchlight, using a 106 Recoilless Rifle mount on a 1/4-ton truck is excellent for this purpose).

d. Emergency lighting. This system may duplicate any or all of the above systems. Its use is limited to times of power failure or other emergencies which render the normal system inoperative. It depends on an alternaative power source, such as installed or portable generators, or batteries.

6-7 Other Lighting

a. Fenced perimeters.

(1) Isolated fenced perimeters are fence lines around areas where the fence is 100 feet or more from buildings or operat-

ing areas, plus the approach area is clear of obstruction for 100 or more feet outside the fence and is not used by other personnel. Both glare projection and controlled illumination are acceptable for these perimeters. Patrol roads and paths should be kept unlighted.

(2) Semi-isolated fenced perimeters are fence lines where approach areas are clear of obstruction for 60 to 100 feet outside the fence and the general public or installation personnel seldom have reason to be in the area. Patrol roads and paths should be kept in relative darkness.

(3) Nonisolated fence perimeters are fence lines immediately adjacent to operating areas within the installation, other installations or to public thoroughfares, where outsiders or installation personnel may move about freely in the approach area. The width of the lighted strip in this case depends on the relative clear zone inside and outside the fence. It may not be practicable to keep the patrol area dark.

b. Building face perimeters consist of faces of buildings on or within 20 feet of the property line or area line to be protected, and where the public may approach the buildings. Guards may be stationed inside or outside of the buildings. Doorways or other insets in the building's face should receive special attention for lighting to eliminate shadows.

c. Active entrances for pedestrians and vehicles should have two or more lighting units with adequate illumination for recognition of persons and examination of credentials. All vehicle entrances should have two lighting units located to facilitate complete inspection of passenger cars, trucks, and freight cars as well as their contents and passengers. **Semiactive and inactive entrances** should have the same degree of continuous lighting as the remainder of the perimeter, with standby lighting of sufficient illumination to be used when the entrance becomes active. Gate houses at entrances should have a low level of interior illumination to enable guards to see better, increase their night vision adaptability and avoid making them targets.

d. Areas and structures within the installation property line consist of yards, storage spaces, large open working areas, piers, docks, and other sensitive areas and structures.

(1) Open yards (defined as unoccupied land only) and outdoor storage spaces (defined as material storage areas, railroad sidings, motor pools, and parking areas) should be illuminated as follows:

(a) An open yard adjacent to a perimeter (between guards and fences) should be illuminated in accordance with the illumination requirements of the perimeter. Where lighting is deemed necessary in other open yards, illumination should not be less than 0.2 foot candle at any point.

(b) Lighting units should be placed in outdoor storage spaces to provide an adequate distribution of light in aisles, passageways, and recesses to eliminate shadowed areas where unauthorized persons may conceal themselves.

(2) Piers and docks located on an installation should be safeguarded by illuminating both water approaches and the pier area. Decks on open piers should be illuminated to at least 1.0 foot candles and the water approaches (extending to a distance of 100 feet from the pier) to at least 0.5 foot candle. The area beneath the pier floor should be lighted with small wattage floodlights arranged to the best advantage with respect to piling. Movable lighting capable of being directed as required by the guards is recommended as a part of the protective lighting system for piers and docks. The lighting must not in any way violate marine rules and regulations (must not be glaring to pilots). The US Coast Guard should be consulted for approval of proposed protective lighting adjacent to navigable waters.

(3) Critical structures and areas should be the first consideration in designing protective fencing and lighting. Power, heat, water, communications, explosive materials, critical materials, delicate machinery, areas where highly classified material is stored or produced, and valuable finished products need special attention. Critical structures or areas classified as vulnerable from a distance should be kept dark (standby lighting available), and those that can be damaged close at hand should be well lighted. The surroundings should be well lighted to force an intruder to cross a lighted area, and any walls should be lighted to a height of 8 feet to facilitate silhouette vision.

6-8 Wiring Systems

Both multiple and series circuits may be used to advantage in protective lighting systems, depending on the type of luminary used and other design features of the system. The circuit should be arranged so that failure of any one lamp will not leave a large portion of the perimeter line or a major segment of a critical or vulnerable position in darkness. Connections should be such that normal interruptions caused by overloads, industrial accidents, and building or brush fires will not interrupt the protective system. In addition, feeder lines should be located underground (or sufficiently inside the perimeter in the case of overhead wiring) to minimize the possibility of sabotage or vandalism from outside the perimeter. The design should provide for simplicity and economy in system maintenance and should require a minimum of shutdowns for routine repairs, cleaning, and lamp replacement. It is necessary in some instances to install a duplicate wiring system.

6-9 Maintenance

a. Periodic inspections should be made of all electrical circuits to replace or repair worn parts, tighten connections, and check insulation. Luminaries should be kept clean and properly aimed.

b. Replacement lamps can be used in less sensitive locations. The actuating relays on emergency lines, which remain open when the system is operating from the primary source, need to be cleaned frequently since dust and lint collect on their contact points and can prevent their operation when closed.

c. The intensity of illumination and specification for protective lighting for fences or other antipersonnel barriers should meet the minimum requirements (next page).

6-10 Power Sources

Power sources should meet the following criteria:

a. Primary— usually a local public utility.

b. Alternate— the following should be provided:

(1) Standby batteries or gasoline-driven generators may be used.

(a) If cost effective, a system should start automatically upon failure of outside power.
(b) Must insure continuous lighting.
(c) May be inadequate for sustained operations, therefore, additional security y precautions must be considered.
(d) Tested to insure efficiency and effectiveness. The frequency and duration of tests depend on:

- Mission and operational factors.
- Location, type and condition of equip ment.
- Weather (temperature affects batteries very strongly).

(2) Located within a controlled area for additional security.

(3) Generator or battery-powered portable and/or stationary lights.

Location	Foot-candles on horizontal plane at ground level
Perimeter of outer area	0.15
Perimeter of restricted area	0.4
Vehicular entrances	1.0
Pedestrian entrances	2.0
Sensitive inner area	0.15
Sensitive inner structure	1.0
Entrances	0.1
Open yards	0.2
Decks on open piers	1.0

Type of area	Type of lighting	Width of lighted strip (ft)	
		Inside fence	Outside fence
Isolated perimeter	Glare	25	200
Isolated perimeter	Controlled	10	70
Semi-isolated perimeter	Controlled	10	70
Non-isolated perimeter	Controlled	20-30	30-40
Building face perimeter	Controlled	50 (total width from building face)	
Vehicle entrance	Controlled	50	50
Pedestrian entrance	Controlled	25	25
Railroad entrances	Controlled	50	50
Vital structures	Controlled	50 (total width from structure)	

Lighting Specification Table

(a) For use in a complete power failure
(b) Includes alternate power supply
(c) Available at designated control points for security personnel.

c. Security— a must.

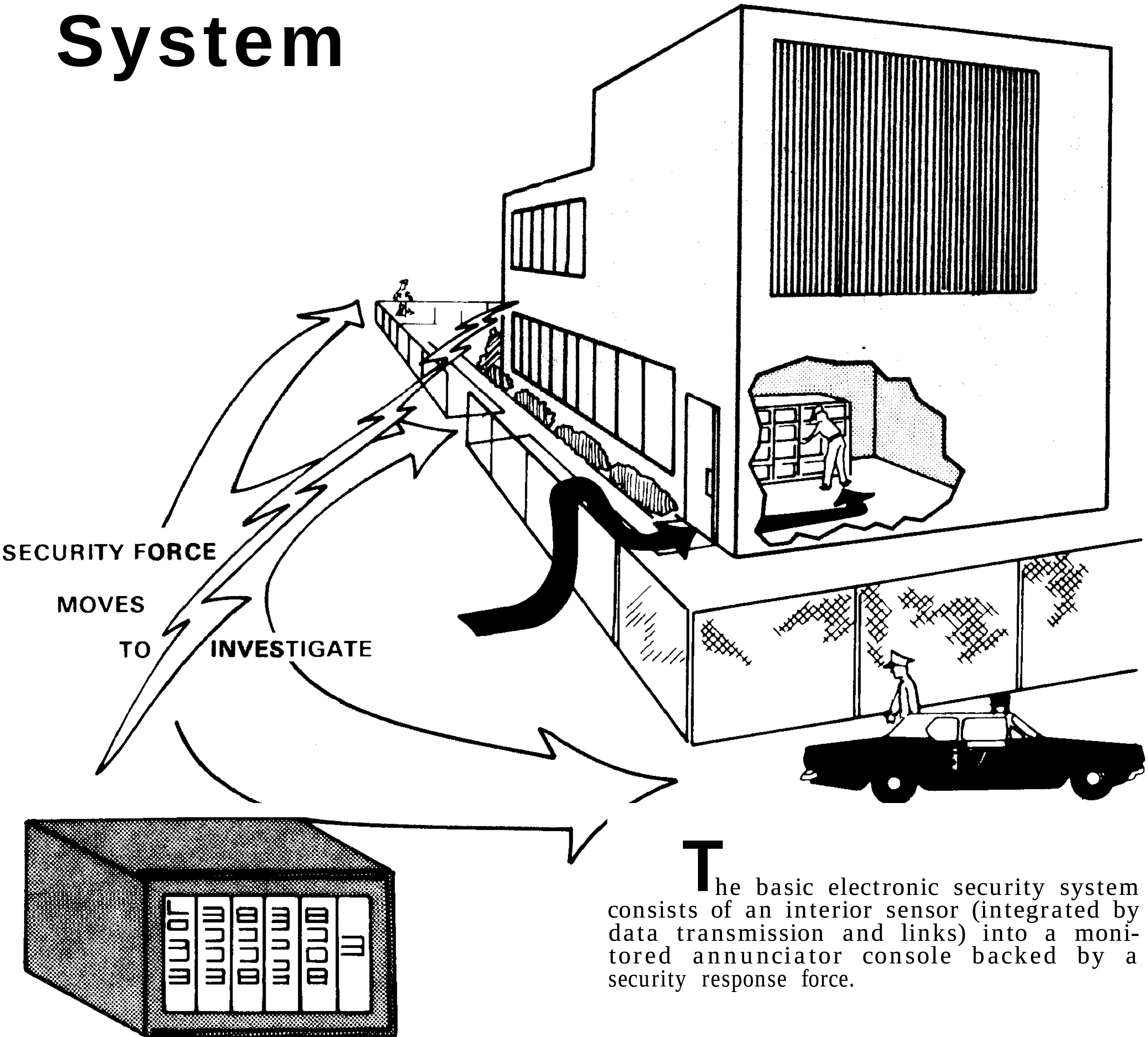
(1) Starts at the points where power feeder lines enter the installation or activity.

(2) Security emphasis goes to sources in terms of mission essential/vulnerable activity, IAW AR 190-13.

(3) Continual physical security inspections of power sources is required to determine security measures and replacement of equipment (transformers, lines, etc.).

Chapter 7

Intrusion Detection System



The basic electronic security system consists of an interior sensor (integrated by data transmission and links) into a monitored annunciator console backed by a security response force.

Intrusion detection systems are an in herent element of the Army's security in depth ring and play a vital part in the overall

protection of military installations, activities, equipment and materiel assets. These systems detect through sound, vibration, motion, electrostatic and/or light beams. Basically, for an item to be secure, the system must focus upon detecting unauthorized individuals at the entry point (gate, door, fence, etc.), area (building, etc.), and at a specific object (vault, file, safe, etc.).

The basic electronic security consists of an interior sensor (integrated by data transmission links) into a monitored annunciator console backed by a security response force.

These systems can be applied to both tactical and nontactical situations. The systems are designed to detect entry of unauthorized persons into the protected area. Individuals responsible for physical security planning must be aware of the advantages and limitations of these systems so they can be incorporated effectively into the security plan.

There are a variety of commercially manufactured and militarily procured systems designed to detect approach or intrusion. Certain systems are suitable only for outdoor protection, while others are suitable only for indoor uses. All have weak points by which their functioning can be minimized or completely interrupted.

It is important for security managers to remember that any detection system is useless unless it is supported by prompt security force action when the system is activated.

The Basics — Section I

7-1 Definitions

The definitions in appendix S are provided for common understanding of intrusion detection systems and their component parts. The definitions apply to commercially produced and militarily procured systems. You will discover that the terms defined may overlap/impinge on other definitions provided or commonly used in the security/intrusion detection field. Some are frequently used in fields other than security, and may have added or different definitions in use. You should review appendix S prior to reading this chapter.

7-2 Technical Review And Approval

Plans and specifications for installation of intrusion detection systems estimated to cost more than $5,000.00 must be forwarded through command channels to: Chief of Engineers (ATTN: DAEN-MCE-D) for final technical review and approval (AR 190-13).

7-3 Purposes

Intrusion detection alarm systems are used to accomplish one or more of the following:

a. Economize — permit more economical

and efficient use of manpower by requiring smaller mobile responding guard forces instead of larger numbers of personnel for patrols and fixed guard posts.

b. Substitute— use in place of other physical security measures which cannot be used because of safety regulations, operational requirements, appearance, layout, cost, or other reasons.

c. Supplement— provide additional controls at critical points or areas.

7-4 Principles of Operation

a. The following are some basic principles upon which intrusion detection systems operate:

(1) Breaking an electrical circuit.

(2) Interrupting a light beam.

(3) Detecting sound.

(4) Detecting vibration.

(5) Detecting motion.

(6) Detecting a change in capacitance due to penetration of an electrostatic field.

b. Each principle is discussed separately in paragraphs 7-7 through 7-12, including advantages and disadvantages.

7-5 Necessity and Feasibility

The following are factors that need to be considered to determine the necessity and feasibility of installing an intrusion detection system.

a. Mission of the installation or facility.

b. Criticality of the installation or facility.

c. Vulnerability of the installation or facility.

d. Accessibility to intruders.

e. Location of installation or facility (geographical) and locations of areas to be protected inside the installation.

f. Construction of building.

g. Hours of operation.

h. Availability of other forms of protection.

i. Initial and recurring cost of the system as compared to cost, in money or security, of possible loss of materials or information.

j. Design and **salvage value** of the system.

k. Response time by the security force.

l. Saving in manpower and money over a period of time.

m. Intruder time requirement.

7-6 Selection

Each type of intrusion detection system is intended to meet a specific type of problem.

a. Factors to be considered in selecting the appropriate components/system include but are not limited to the following:

(1) Location and response time capability of security personnel.

(2) Value of facility, material, or the sensitivity of classified defense material to be protected.

(3) Area environment, to include building construction, sound levels inside and outside, climate, etc.

(4) Radio and electrical interference.

(5) Operational hours of the installation or facility.

(6) Specific target to be protected.

(7) Availability of security personnel.

b. A consideration of these factors readily indicates the advisability of obtaining technical data to assist in making a wise selection. Often more than one type of sensor, or even system is necessary to give adequate protection for an area or structure.

Types of Systems — Section II

7-7 Breaking An Electrical Circuit

a. Possible points of entry into buildings or enclosures can be wired by using electrically sensitized strips of metallic foil or wire. Any action that breaks the foil or wire breaks the electrical circuit and activates an alarm. Metallic foil is frequently used on glass surfaces. Doors and windows may be equipped with magnetic contact switches which sound an alarm when the door or window is opened. Metallic wire running through concealed wooden dowels or between panels or walls, doors, and ceilings may be used.

b. Characteristics:

(1) Advantages. Consistently provides the most trouble-free service; causes few, if any, nuisance alarms. Adequate in low-risk applications.

(2) Disadvantages:

(a) Costly to install where there are many entry points to the protected area.
(b) Easily compromised when improperly applied; unprotected soft walls or ceilings may be penetrated without disturbing the alarm system; it may also be defeated by bridging the circuits.
(c) Has little salvage value–not recoverable.
(d) Will not detect "stay-behinds."

7-8 Interrupting a Light Beam

a. The photoelectric (electric eye) type of intrusion detection derives its name from the use of a light-sensitive cell and a projected-light source.

(1) A light beam is transmitted at a frequency of several thousand vibrations per second. An infrared filter over the light source makes the beam invisible to intruders.

(2) Alight beam with a different frequency (such as a flashlight) cannot be substituted for this beam. The beam is projected from a hidden source and maybe crisscrossed in a protected area by means of hidden mirrors until it contacts a light-sensitive cell.

(3) This device is connected by wires to a control station. When an intruder crosses the beam, he breaks contact with the photoelectric cell, which activates an alarm.

(4) A projected beam of invisible light can be effective for approximately 500 feet indoors and will cover an area up to 1,000 feet outdoors. The effectiveness of the

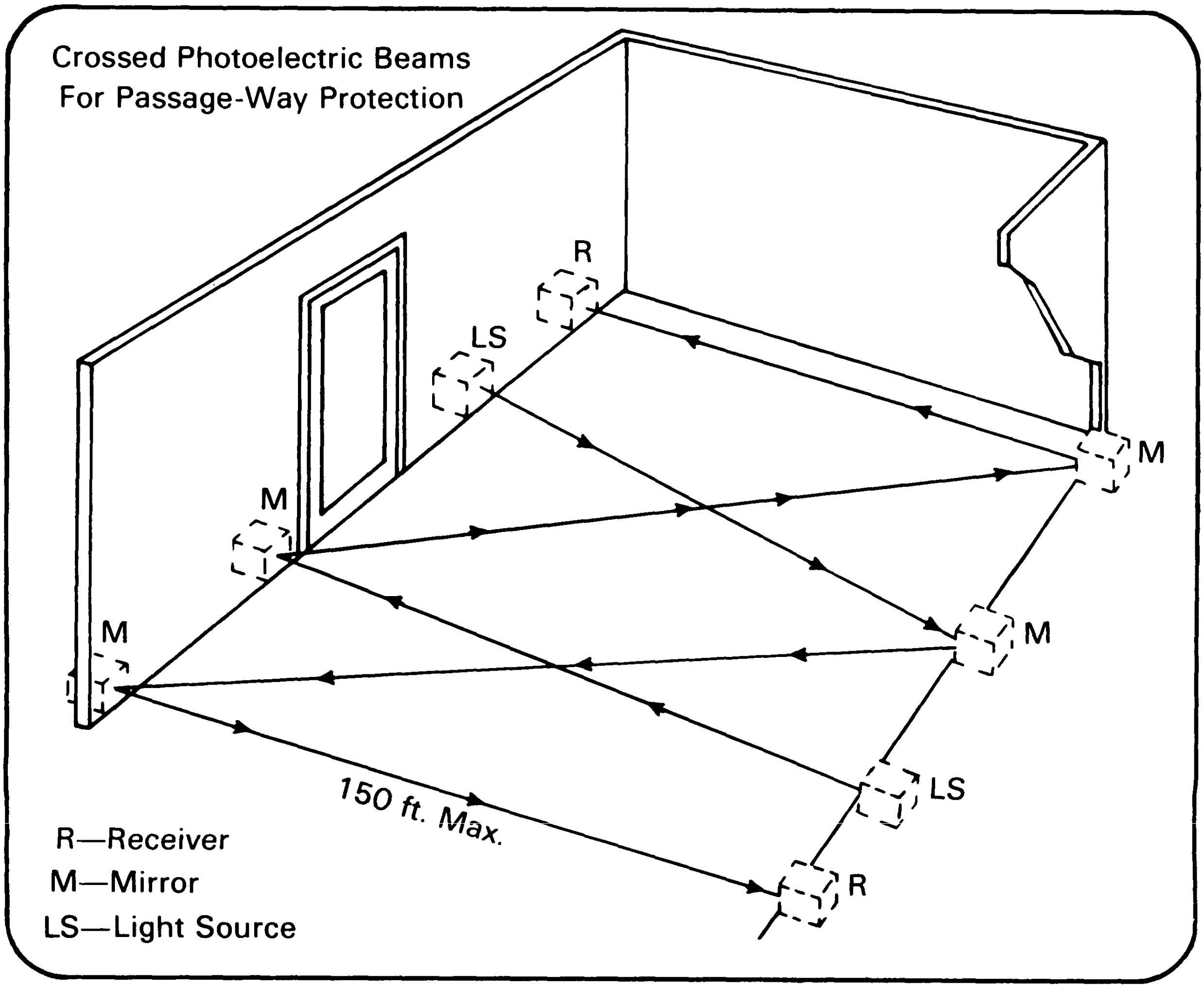


Figure 25—Sample of photoelectric intrusion detection device.

beam decreases from 10 to 30 percent for each mirror used. Figure 25 shows a typical light beam setup.

b. Characteristics.

(1) Advantages.

(a) When properly employed, affords effective, reliable notice of intrusion.
(b) Useful in open portals or driveways where obstructions cannot be used.
(c) Detects "stay-behinds."
(d) Has a high salvage value; almost all equipment is recoverable.
(e) May be used to actuate other security devices, such as cameras.
(f) May detect fires through smoke interruption of the beam.

(2) Disadvantages

(a) Employment is limited to those locations where it is not possible to bypass the beam by crawling under or climbing over it.
(b) Requires some type of permanent installation.

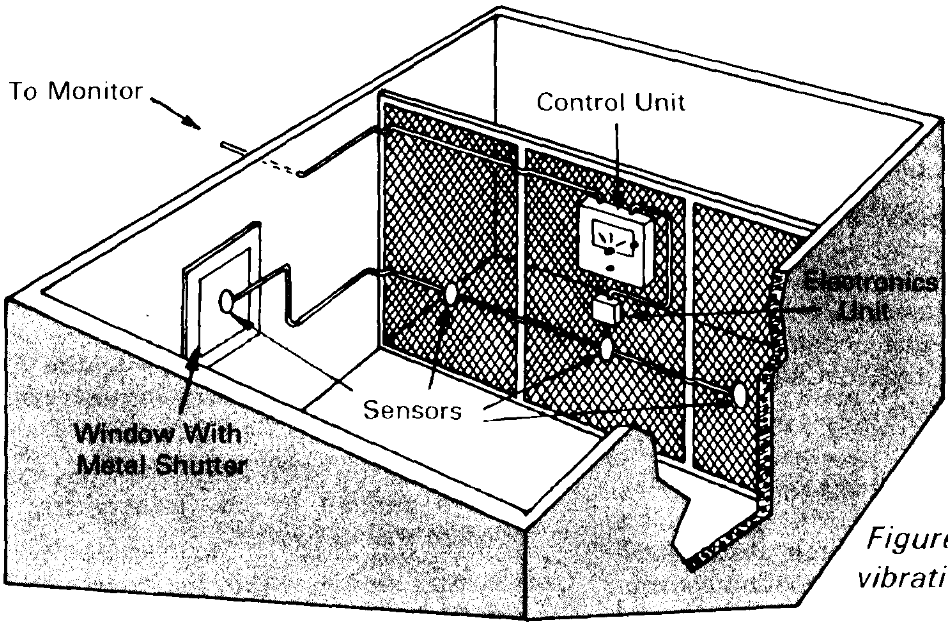


Figure 26—Example of vibration sensor setup.

(c) Fog, smoke, dust, and rain in sufficient density will cause interruption of the light beam.
(d) Requires frequent inspections of light producing components to detect deterioration.
(e) Requires keeping the ground beneath the light beam free of tall grass, weeds, drifting snow, and sand.

7-9 Detecting Sound

a. This type of intrusion detection system can be effectively used to safeguard enclosed areas, vaults, warehouses, and similar enclosures. Supersensitive microphone speaker sensors are installed on walls, ceilings, and floors of the protected area. Any sound caused by attempted forced entry is detected by the sensor. Sensitivity can be adjusted.

b. Characteristics.

(1) Advantages.

(a) Economical and easily installed.
(b) High salvage value.
(c) Microphone speakers may be used in more expensive sensors to monitor sounds coming from the protected area.

(2) Disadvantages. Can be used only in enclosed areas where a minimum of extraneous sound exists; not satisfactory where high noise levels are encountered, especially in proximity to aircraft and railroad traffic. Cannot be used effectively outdoors. Should not be used in areas where sensitive classified discussions occur unless the system is designed to prevent its use as a clandestine listening device.

7-10 Detecting Vibration

This type of intrusion detection system can be effectively used to safeguard enclosed areas in sound detection systems.

a. Vibration-sensitive sensors are attached to walls, ceilings, and floors of the protected area. Any vibration caused by attempted forced entry is detected by the sensors. Sensitivity can be adjusted. (See figure 26 for a sample setup).

b. Characteristics:

(1) Advantages.

(a) Economical and easily installed.
(b) High salvage value.
(c) Flexible application.

(2) Disadvantages. Can be used only in areas where a minimum of vibration exists; not satisfactory where high vibrations are encountered, especially in proximity to heavy construction, railroad, or automotive/truck traffic. Cannot be used effectively outdoors.

7-11 Detecting Motion

a. Intrusion detection systems using ultrasonic or microwave motion sensors can be very effective for the protection of interior areas. Such systems flood the protected area with acoustic or microwave energy and detect the Doppler shift in transmitted and received frequencies when motion occurs within the area.

b. Ultrasonic systems consist of transceivers (single unit containing a transmitter and receiver or separate transmitters and receivers), and electronic unit (amplifier) and a control unit.

(1) The transmitter generates a pattern of acoustic energy which fills the enclosed area.

(2) The receiver, connected to the electronic unit, picks up the standing sound patterns.

(3) If they are of the same frequency as the waves emitted by the transmitter, the system will not alarm.

(4) Any motion within the protected area sends back a reflected wave differing in frequency from the original transmission. The change in frequency is detected, amplified, and the alarm signal activated (illustrated example in figure 27).

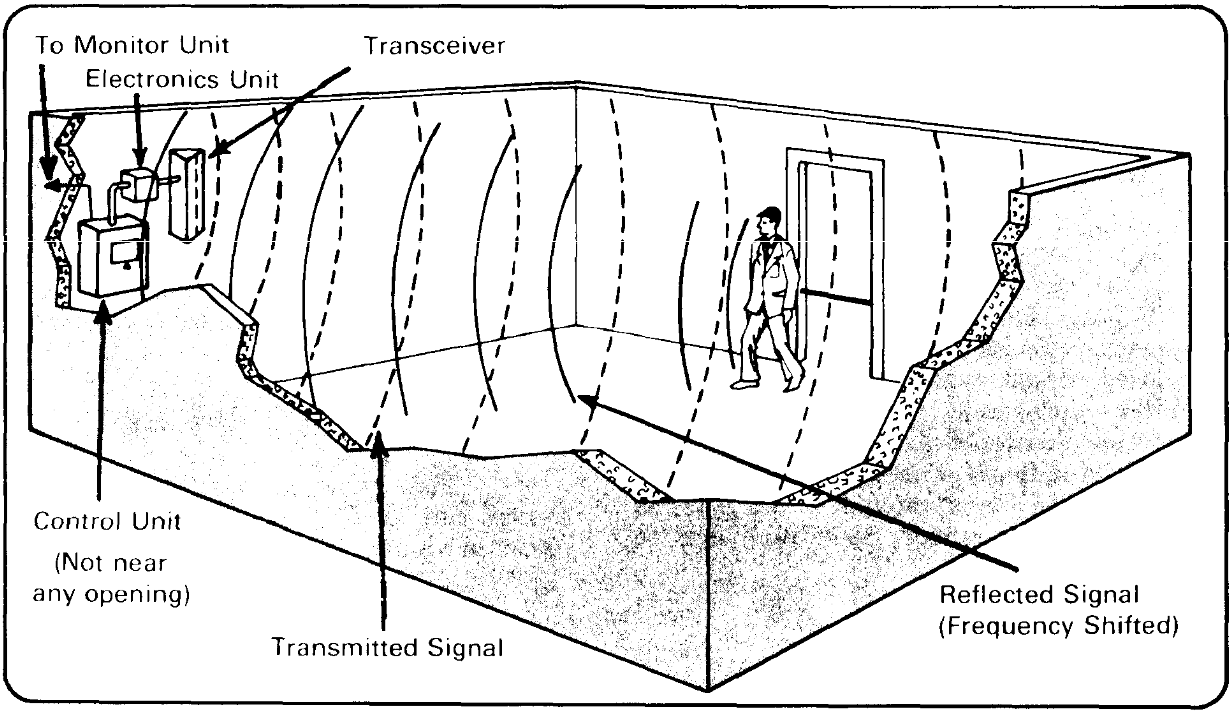


Figure 27—How an ultrasonic motion sensor works.

(5) Multiple transceivers or a transmitter and multiple receivers may be operated from the same control unit for more effective coverage of large or broken areas. This system can only be used indoors.

(6) Advantages.

(a) Provide effective security protection against intruders concealed within the premises.
(b) High salvage value.
(c) Protective field is not visible, therefore, it is difficult to detect the presence of, or to compromise the system.

(7) Disadvantages.

(a) May require reduced sensitivity to overcome possible disturbance factors in the enclosed area (such as telephones, machines, clocks, etc.).
(b) Can be set off by loud external sounds.

c. Microwave systems closely parallel the operation of ultrasonic systems. A pattern of radio waves is transmitted and partially reflected back to an antenna. If all objects within the range of the radio waves are stationary, the reflected waves return at the same frequency. If they strike a moving object, they return at a different frequency. The difference in the transmitted and received frequency is detected, thus initiating an alarm signal.

(1) Advantages.

(a) Good coverage is provided if antennas are properly placed.
(b) Not affected by air currents, noise, or sound.
(c) High salvage value.

(2) Disadvantages.

(a) Coverage is not easily confined to desired security area. Penetrates thin wooden partitions and windows and therefore may be accidentally activated by persons or vehicles outside the protected area.
(b) Fluorescent light bulbs will activate the sensor.

7-12 Detecting Capacitance Change In An Electrostatic Field

a. The capacitance or electrostatic intrusion detection system can be installed on a safe, wall, and/or openings therein in an effort to establish an electrostatic field around the object to be protected. This field is tuned by a balance between the electric capacitance and the electric inductance. The body capacitance of any intruder who enters the field unbalances the electrostatic energy of the field. This unbalancing activates the alarm system. (See figure 28, next page.)

b. Characteristics:

(1) Advantages.

(a) Extremely flexible type of system; it may be used to protect safes, file cabinets, windows, doors, partitions; in fact any unguarded metallic object within maximum tuning range may be protected.
(b) Simple to install and operate.
(c) Provides an invisible protective field, making it difficult for an intruder to determine when system has been set off.
(d) High salvage value-may be easily dismantled and reinstalled.
(e) Compact equipment size.
(f) High grade of protection.

(2) Disadvantages.

(a) Can be applied only to ungrounded equipment.
(b) Housekeeping of protected area on object must be carefully watched.
(c) Accidental alarms can occur if protected area or object is carelessly approached, such as by porters or cleaners at night.

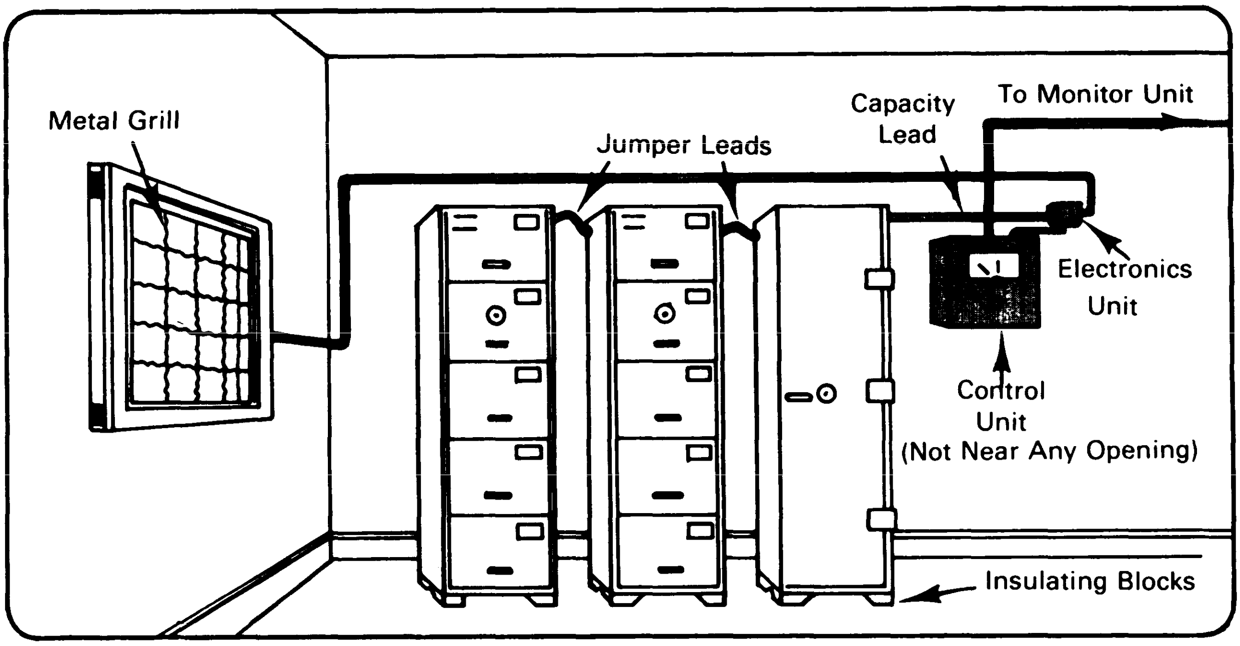


Figure 28—Example of capacitance proximity sensor setup.

7-13 Penetration Sensors

Modern penetration alarm sensors can be used at any installation or activity for additional security protection. Their versatility lends to use on windows, interior or exterior doors, ceilings, walls and other potential entry areas.

a. Exterior doors. To guard against unauthorized entry, the door can be equipped with one or more balanced magnetic switches as shown in figure 29. The surface of an interior door or wall can be covered with a grid wire sensor (figure 30) or any type system using the principle of breaking an electrical circuit, as discussed in paragraph 7-7 of this chapter.

b. Interior doors. These sensors are subject to the same considerations that govern the choice of systems for exterior doors.

c. Solid walls, floors and ceilings. To monitor attempts to penetrate solid walls, floors, and ceilings, the interior surface may be covered with a grid wire sensor, or the room equipped with a passive ultrasonic sensor (see figure 31, page 102). Sound detection systems (par. 7-9) and vibration detection systems (par. 7-10) may also be used to detect penetration through such areas.

d. Open walls and ceilings. Wire cage walls and ceilings present distinct problems. To protect this type of construction, certain modifications are necessary. The wall and ceiling may be enclosed with building material on the outside of the cage. This permits use of passive ultrasonic or grid wire sensors.

e. Windows. Wherever possible, windows should be eliminated. Where windows are necessary, consider the use of interior metal shutters which can be closed and locked. This allows use of passive ultrasonic sensors. If the character of the room does not allow the use of a passive ultrasonic sensor, the vibration sensor (par. 7-10) or capacitance proximity sensor (par. 7-12) can be used instead. Any system using the principle of breaking an electrical circuit can also be considered.

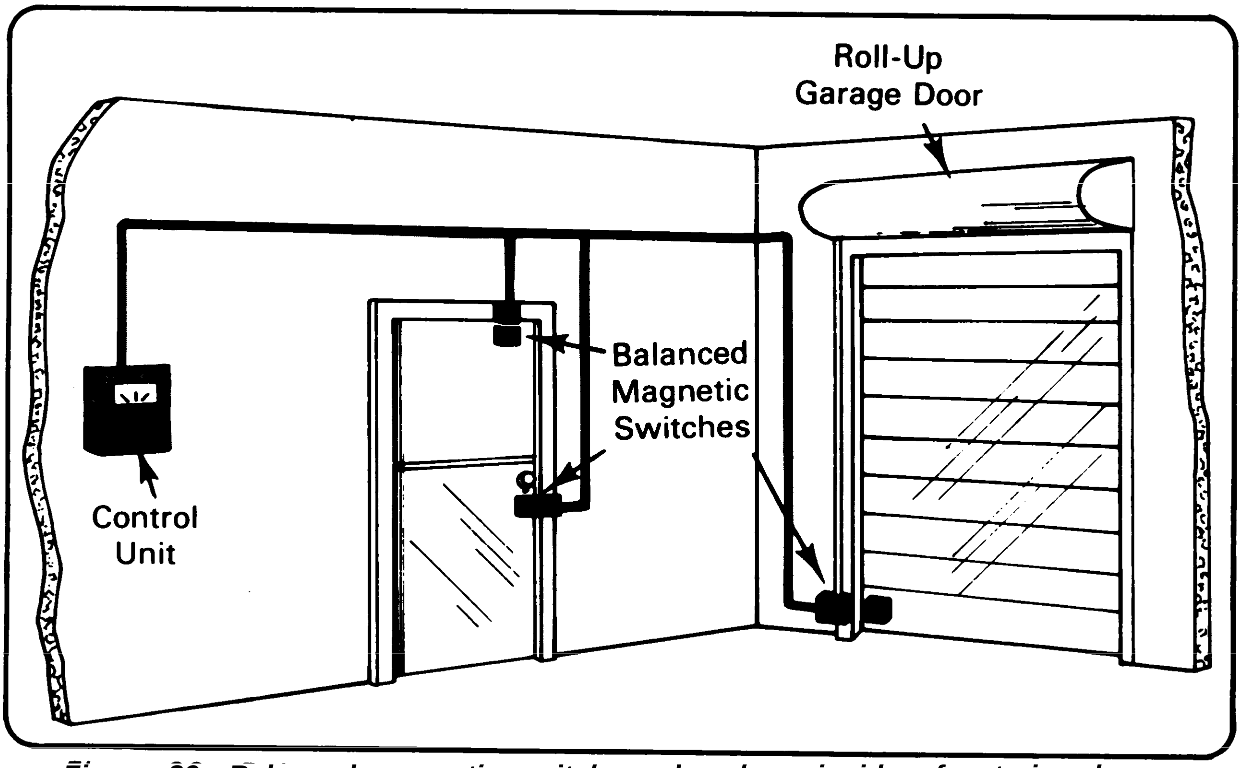


Figure 29—Balanced magnetic switches placed on inside of exterior doors.

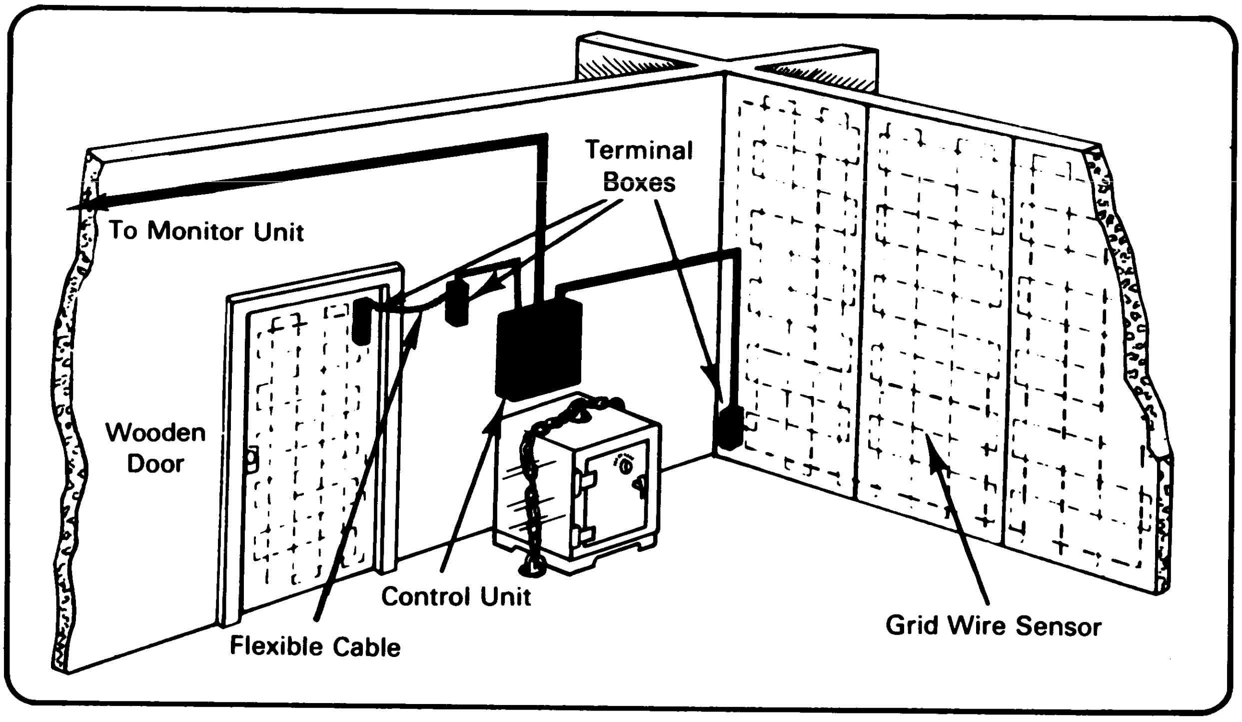


Figure 30—Grid wire sensors used on interior surfaces.

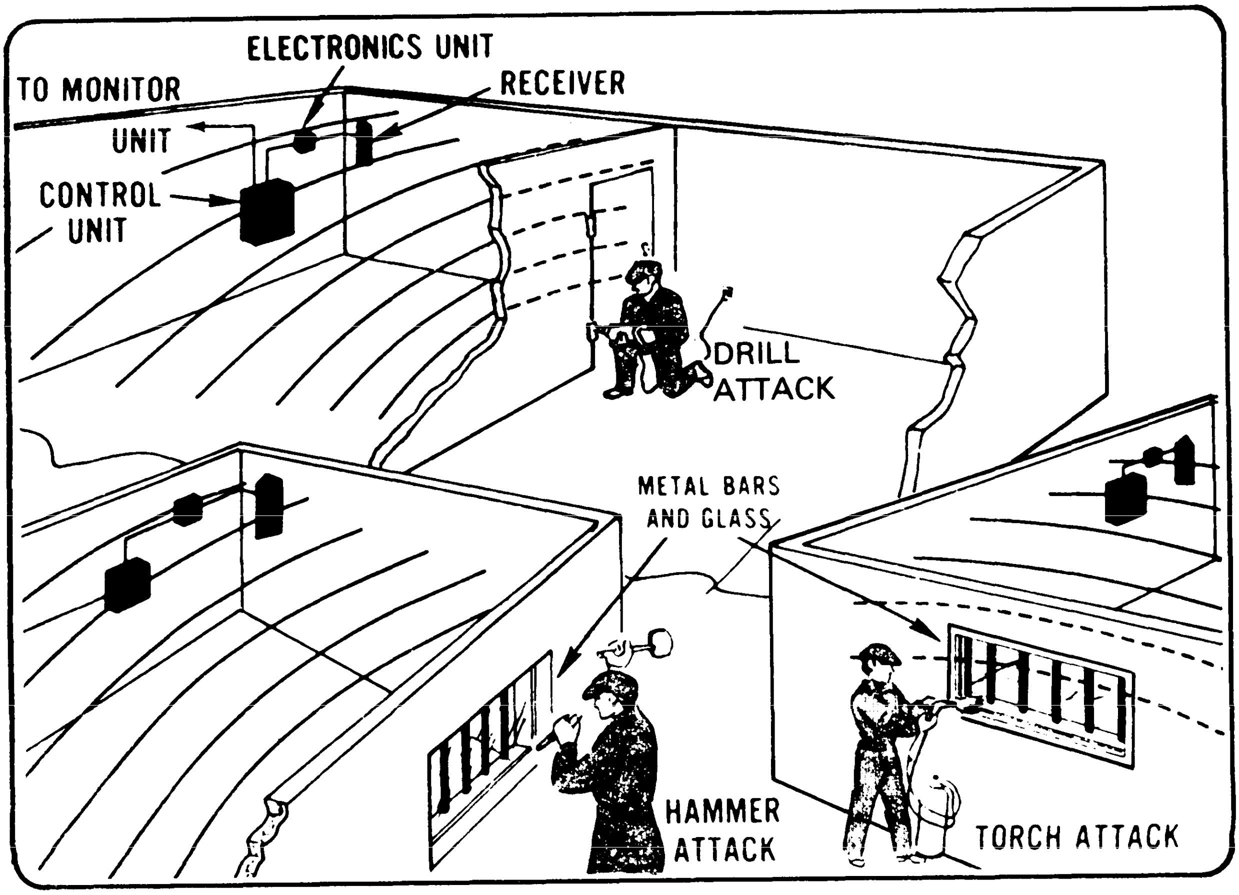


Figure 31—Examples of passive ultrasonic sensor effectiveness.

f. Ventilation openings. These are any openings in the ceiling, walls, or doors to allow the free passage of air. They are generally covered with steel bars, mesh, or louvered barriers. For maximum protection, you should consider eliminating ventilators. Where it is not possible to seal ventilators, consider the use of locked metal shutters. Intrusion through the ventilators then can be detected with the passive ultrasonic sensor or the vibration sensor. Where the ventilators are required to be open all the time, a metal grill can be placed over the inside of the ventilator opening and the capacitance proximity sensor can be used.

g. Construction openings. These are unsecured openings from incomplete construction. The openings can be covered with a grid wire sensor installed on plywood. Where the opening is required to stay open, a capacitance proximity sensor can be used on the inside of the opening.

h. Air conditioners. To monitor for intrusion through an air conditioner aperture, the capacitance proximity sensor can be used on a metal grill extending into the room in front of the unit.

7-14 Motion Sensor

To detect the motion of an intruder inside a protected area, an ultrasonic motion sensor (par. 7-11) can be used, provided there

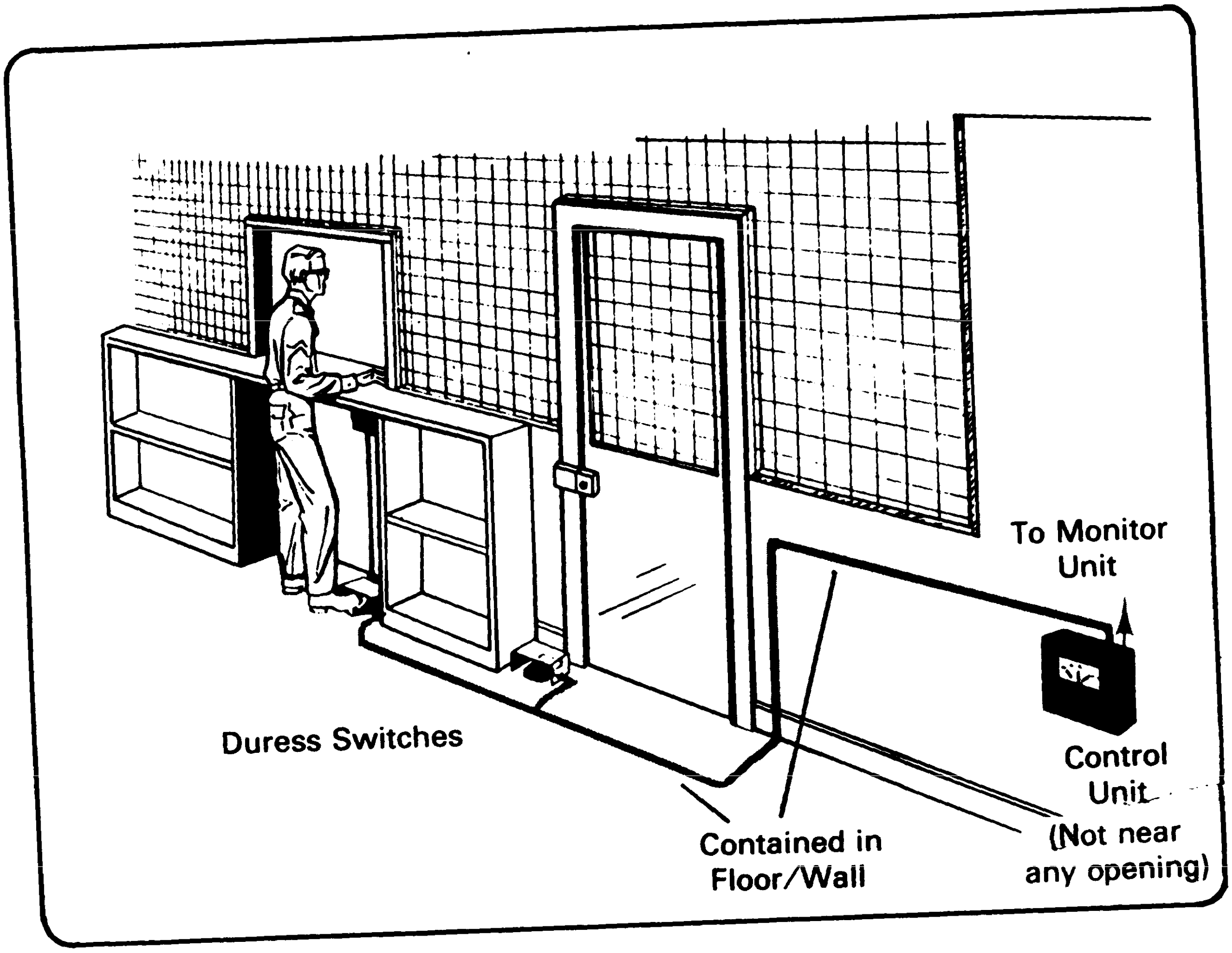


Figure 32—Examples of fixed duress sensor placement.

is a minimal flow of air from heating units, air conditioned, cracks in the protected area, or any other possible source of air turbulence, as this may reduce the effectiveness of the sensor or cause nuisance alarms. A microwave system (par. 7-11) may also be used to protect an enclosed area.

7-15 Duress Sensor Considerations

Fixed. This sensor is used to call for assistance of other personnel. It consists of a foot- or hand-operated switch located in a position most likely to be occupied by personnel working in the protected area (figure 32).

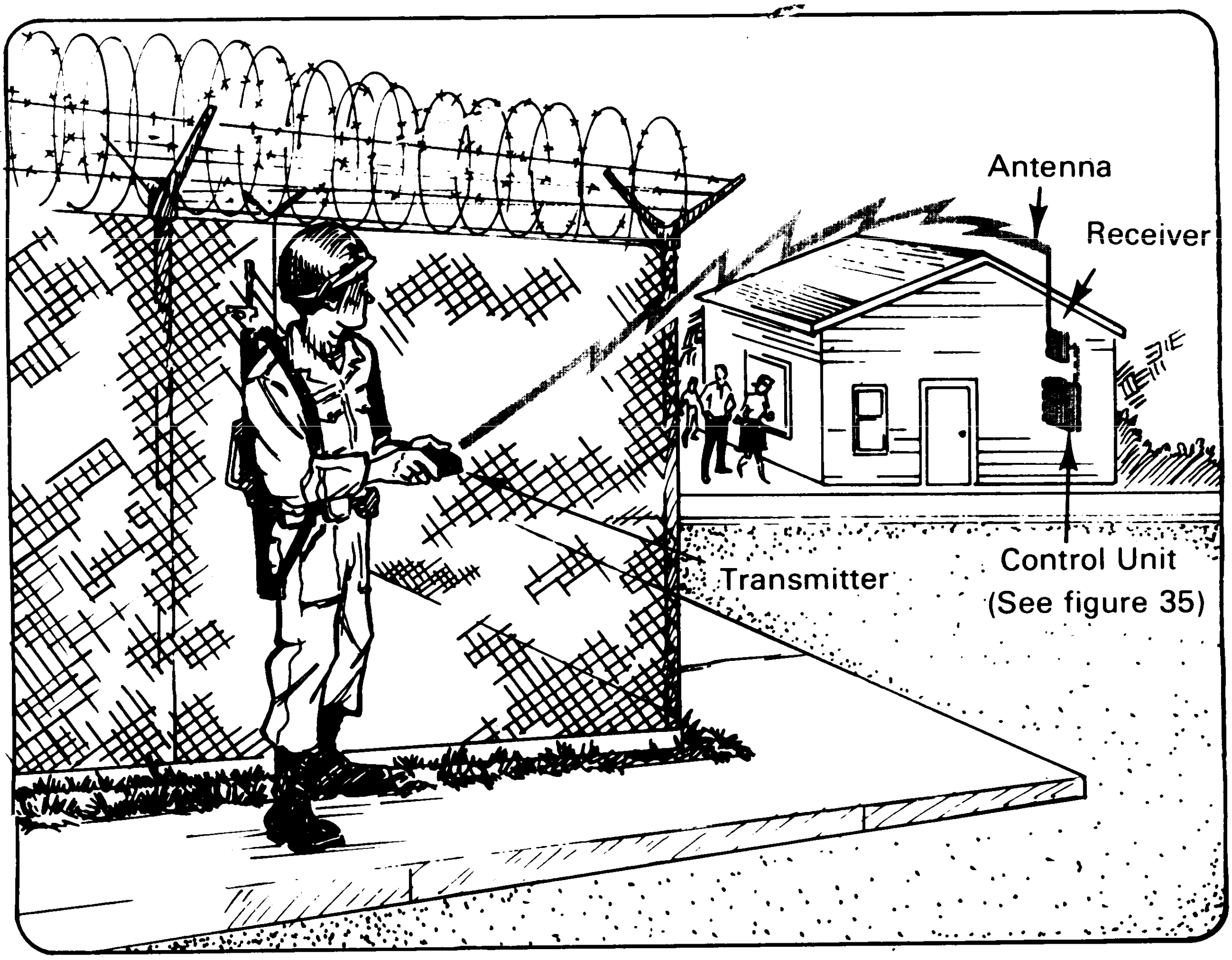


Figure 33—Examp/e of portable duress sensor use.

Portable. An alternate to the fixed duress sensor, the portable duress sensor is a UHF transmitter which can send an alarm to a receiver located at the control unit. The effective range will be restricted depending upon inside or outside use (figure 33).

7-16 Point Sensor Considerations

a. Storage cabinets and safes. To detect movement near to or contact with any part of a storage cabinet or safe, the capacitance proximity sensor can be used.

b. Weapons. To detect removal of weapons from a standard weapons rack, a magnetic weapon sensor (figure 34) can be used. (Also see Section IV, The Systems, for security of arms and ammunition.)

7-17 Control Unit

One control unit (figure 35) is required in each secure area to receive signals from the sensors and to transmit signals to the monitor unit and local audible alarm.

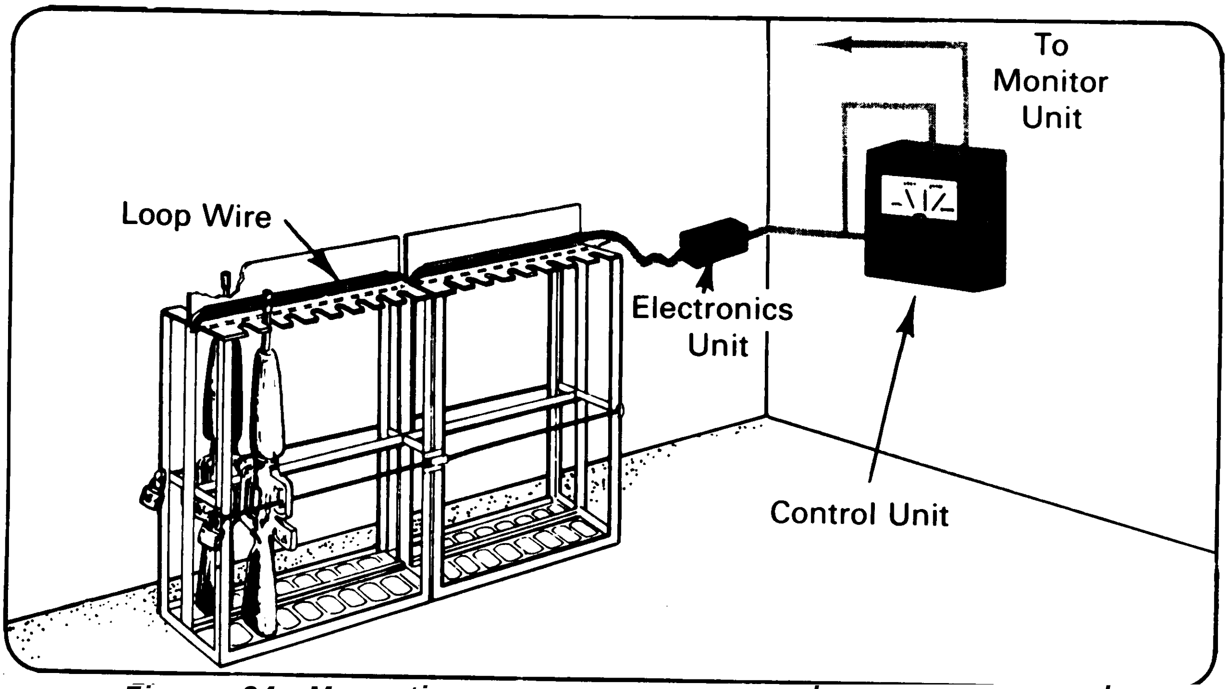


Figure 34—Magnetic weapons sensor used on weapons rack.

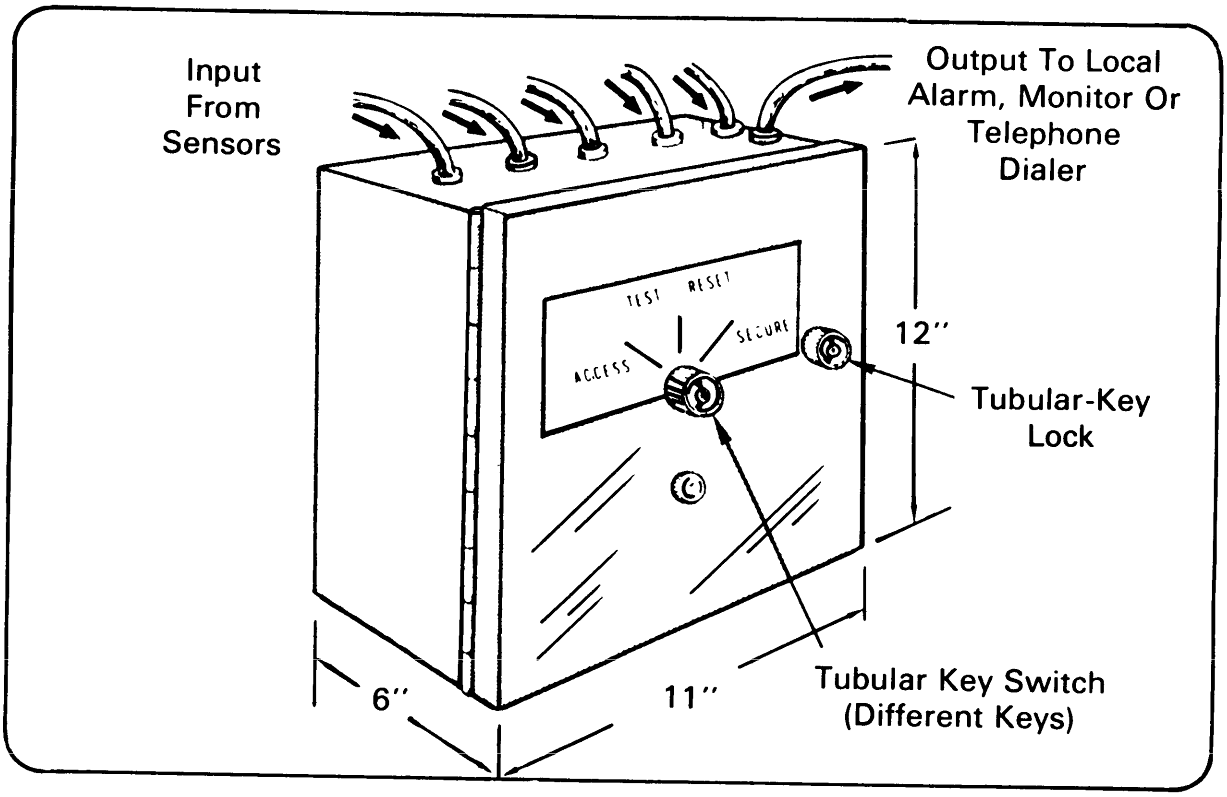


Figure 35—Sample details of control unit.

153-846 0 - 94 - 7

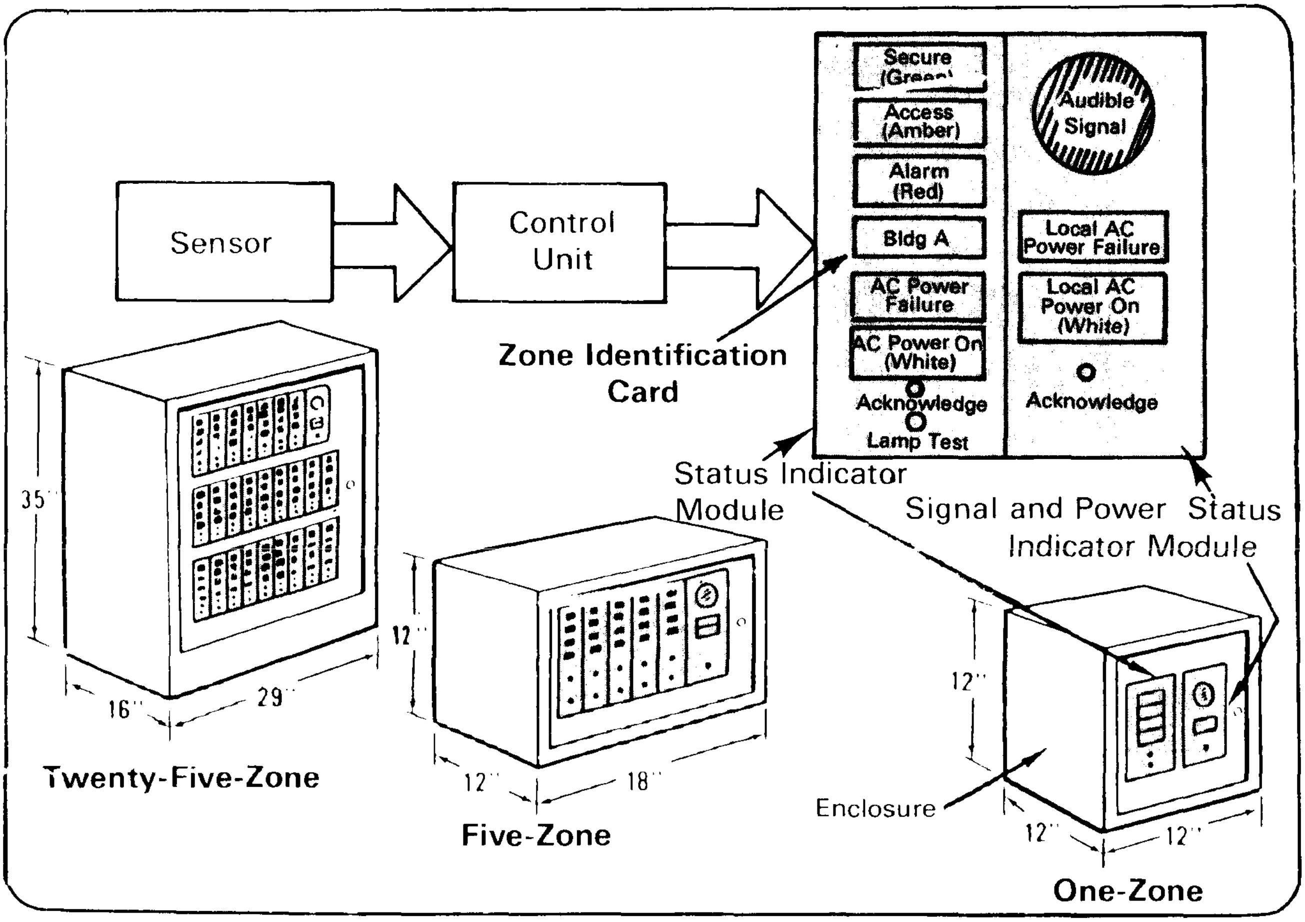


Figure 36—Monitor unit examples.

7-18 Monitor Unit

Each control unit must report to a separate monitor unit status indicator module (see figure 36). Each monitor unit must contain one signal and power status indicator module.

7-19 Local Audible Alarm

A local audible alarm (see figure 37) may be installed outside the protected area. This alarm serves two purposes. Initially, it may scare the intruder away. Secondly, it alerts local guard and police forces in the area. This alarm has limited value for areas where there are no response personnel. A local audible alarm should not be used without a remote monitor unit.

7-20 Telephone Dialer

A telephone dialer (figure 38) maybe employed where it is not possible to install a monitor unit. This device telephones an alarm to a number of preselected phones. Telephone dialers are recommended only for low-security application. Telephone dialer lines may be tied up by calling the number which receives the alarm notification message. They are subject to other tampering and interruption and do not alarm when they are out of order, cut, or grounded.

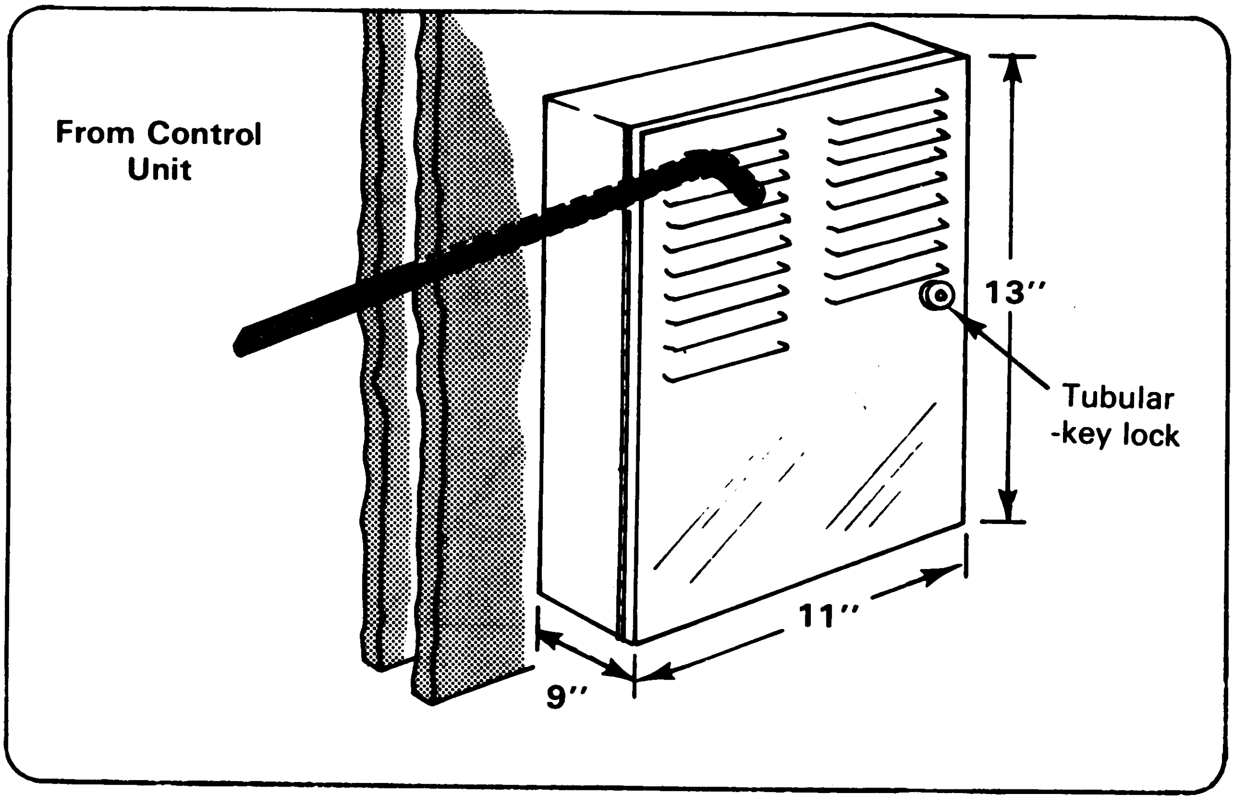


Figure 37—Example of local audible alarm.

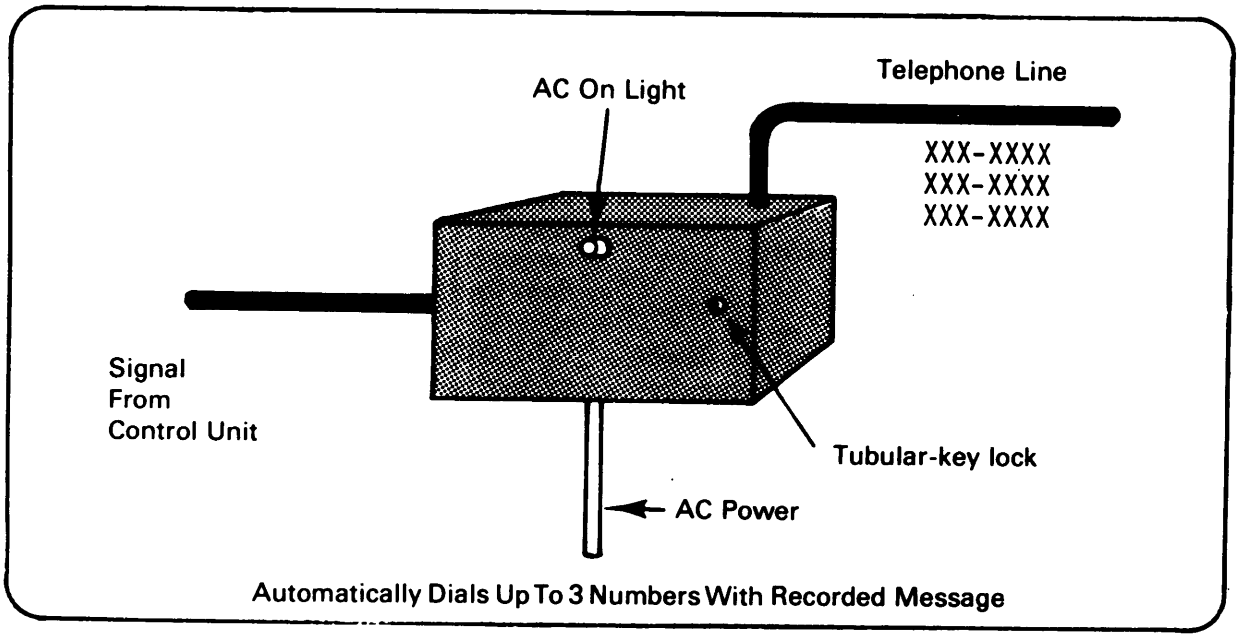


Figure 38—Telephone dialer example.

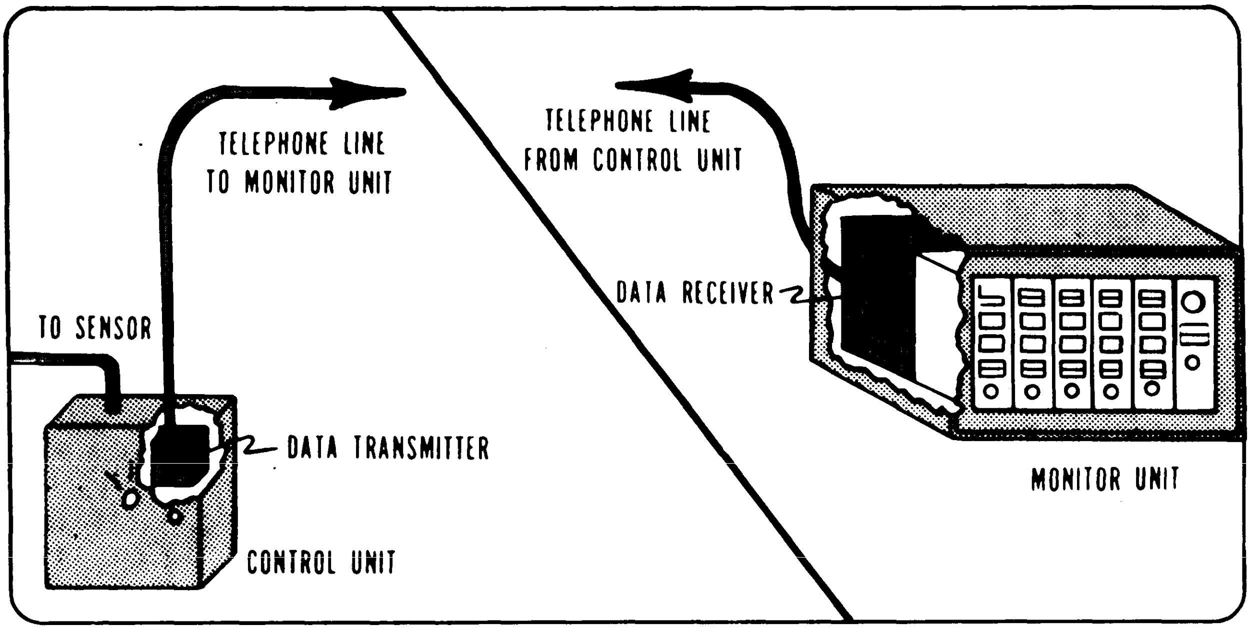


Figure 39—Example of data transmission system.

7-21 Data Transmission System (Type I

The data transmission system (figure 39) is used wherever there are segments of the signal transmission line accessible to tampering, or wherever the signal is transmitted over commercial conductors. One data transmission system is required for each security zone covered by a control unit connected to such a line.

7-22 Intrusion Detection Alarm Report

Alarm and communications detection systems are closely allied in any comprehensive protection system. Telephone and radio communications are so common in everyday usage that their adaptation to a protective system poses few new problems. An alarm detection system is simply a manual or automatic means of communicating a warning of potential or present danger. Types of alarm detection systems include the following:

a. Local alarm system. In a local alarm system the protective circuits or devices actuate a visual or audible signal in the immediate vicinity of the object of protection. Response is by the local security force or other personnel within sight or hearing. The light or sound device should be displayed on the exterior of the building, and should be fully protected against weather or willful tampering. It should be connected to the control element by a tamperproof cable, and should be visible or audible for a distance of at least 400 feet. This system can also be used in conjunction with a proprietary system, as described in paragraph 7-22d.

b. Auxiliary system. An auxiliary system is one in which the installation-owned system is a direct extension of the civil police and/or fire alarm systems. This is the least effective system and because of dual responsibility for maintenance is not favorably considered by many protective organizations.

c. Central station system. A commercial agency may contract to provide electric

protective services to its clients by use of a central station system. The agency designs, installs, maintains, and operates underwriter-approved systems to safeguard against fire, theft, and intrusion; and monitors industrial processes. Alarms are transmitted to a central station outside the installation from which appropriate action is taken such as notifying local police or fire departments.

Note. Direct connected systems or central station systems may be appropriate for armories/buildings used by the Army National Guard, Army Reserve, and/or Army ROTC. The main consideration is lack of an organic or supporting response force.

d. Proprietary System. A proprietary system is similar to the central station system except that it is owned by, and located on, the installation. Control and receiving equip ment is located in the installation security or fire department headquarters. Response to an alarm is by the installation's own security or firefighting personnel. In addition, this type of system may be connected with the civil police and fire departments, and with a commercial central station.

7-23 Signal Transmission Lines

An intrusion detection system is no better than the security of the conductors that transmit the alarm signal to the monitor unit. These conductors must be sensitive enough to cause an alarm in the event of tampering.

a. An intrusion detection system may be defeated regardless of the effectiveness of its sensor if the signal transmission line is not functioning properly. Conductors may be made ineffective by an intruder who has sufficient knowledge of electricity and the necessary equipment to adjust the resistance in the signal transmission lines.

b. Signal transmission lines maybe supervised in a variety of ways, according to location of the lines and the security required.

(1) The simplest means of line supervision is to monitor whether an electrical circuit has been broken, grounded, or shorted.

(2) The most common means is to monitor whether a predetermined variation to an electrical current has occurred. For example, an alarm light might be created if a 30-milliamp current has been increased or decreased five percent.

(3) A more sophisticated means is to monitor two or more features of a complex signal, such as current and frequency. If the signal is changed on a random basis, the likelihood of the signal being recorded and replayed successfully is very remote.

(4) Another approach is to monitor a digital- or tone-type signal transmitted through a telephone system. An investigation and reply scheme is ordinarily employed. Since an electrical current is not being monitored in this case, the distance limitation (a few miles) of the other types does not apply.

c. The need for constant electronic or other type surveillance of signal transmission lines must be emphasized to insure awareness of security personnel that this is normally the weakest link in the system. Emphasis must also be placed on the necessity to maintain records of both nuisance alarms and scheduled/unscheduled maintenance to insure proper operation of the system at all times.

d. Signal transmission lines can be secured by locating them on high overhead poles, burying them, leading into buildings as high as possible, locking terminal cabinets, and comparable measures.

Protective communication systems vary in size and type with the importance, vulnerability, size, location, radio receptivity, and other factors affecting a specific installation, and must be largely subject to local determination.

7-24 Primary Communication Systems

In many situations, the regular communication system of an installation is not adequate for protective security purposes. It is desirable for security forces to have their own communication system with direct lines outside and an auxiliary power supply. Although principal dependence is on the telephone and the teletype, interior and exterior radio communications play an important part in the protective net of large installations.

One or more of the following means of communication should be included in the protective system.

a. Facilities for local exchange and commercial telephone service.

b. Intraplant, interplant, and interoffice teIephone systems using either Government-owned or rented circuits and equipment; but not interconnected with facilities for commercial exchange or toll telephone service.

c. Radiotelephone and\or radiotelegraph facilities for either point-to-point or mobile service.

d. Telegraph and teletype facilities for either commercial service or private line operation.

e. Hand-carried portable radios and\or receivers, with transmitters stationed strategically throughout the installation.

f. A security supervisory system consists of key-operated electric call boxes located strategically throughout an installation. By inserting the key in the call box, security personnel can make routine tour reports or summon emergency assistance. Tampering with the transmitting key or the call box automatically locks the latter, causing a failure of the signal. This signal failure would prevent future routine/scheduled calls, a cause sufficient for immediate investigation.

7-25 Alternate Communication Systems

Alternate communication systems must be provided for use in emergencies. The flood of inquiries that follow emergency conditions added to the normal flow of messages may, overload the existing system at the very time that sure and rapid communication is vital. The most efficient emergency reporting system consists of direct connection to the security or communications center from telephones strategically placed throughout the installation. The use of these telephones should be restricted to emergencies and security force reporting only. The wires of alternate communication systems should be separated from other communication lines,

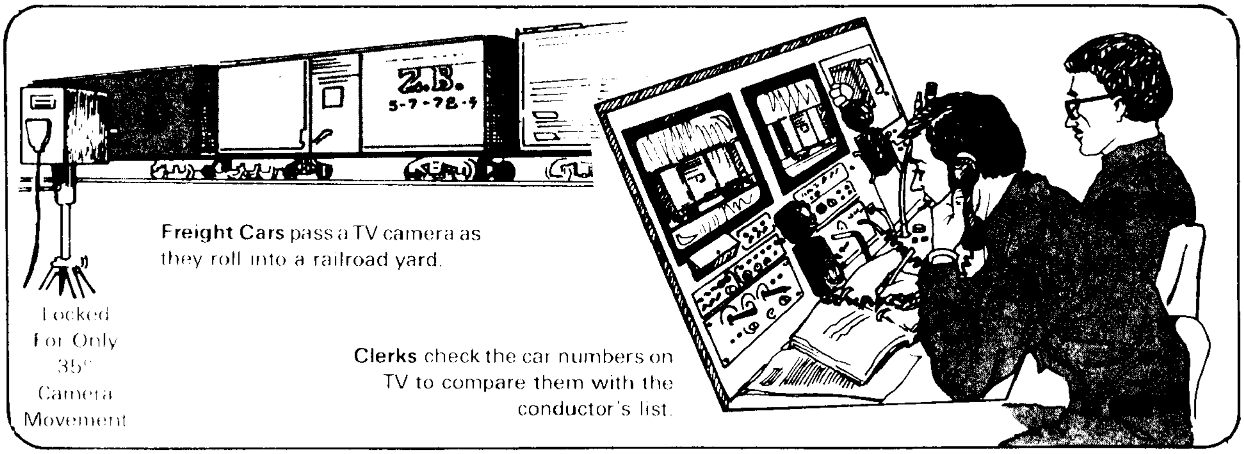


Figure* 40—TV *monitoring of cargo movement.

and should be in underground conduits. For emergency communication with agencies outside the installation, leased wires or a radio adjustable to civil police and fire department frequencies should be available.

7-26 Wiring, Inspection, And Testing

a. Whenever practicable the signal transmission lines of communications systems should be on separate poles or in separate conduits from the installation com - munication and lighting system.

b. Tamper resistant. wire and cable. with she ath of foil that transmits a signal when penetrated or cut, provides added protection.

c. All communication circuits should be tested at least, onto during each tour of duty, preferably when the new shift assumes duty. At small installations that do not employ security forces, a test should be made immediately before closing for the night. Some commerically manufactured systems have self-testing features which should be checked periodically by the security patrol or operating force. All equipment must be inspected periodically by the technical maintenance personnel who will repair or replace worn or failing parts.

7-27 Closed Circuit Television

Closed circuit television (CCTV), while not an intrusion detection system in itself, is very useful in physical security operations and is frequently used to complement such a system.

a. This may be accomplished by placing cameras at critical locations to provide direct visual monitoring from a vantage point. Closed circuit television may be used on gates or other security areas not manned continuously. This system normally consists of a television camera, monitor, and electrical circuitry. The camera may be remotely controlled by monitoring security personnel.

b. Normal use of TV on entry points includes the use of a two-way communication system between the monitor panel and the gate, and an electrically operated gate lock. With this device, the person at the monitor panel can be alerted on the speaker system by a person desiring to enter, converse with the person, observe him on the monitor to determine his authority to enter, and then release the gate lock. An adaptation may be added to this equipment to enable the monitor personnel to make a side-by-side comparison of a person's face with the picture of his identification badge.

c. CCTV can also be used for surveillance of security cages, high value goods in warehouses, fence lines, movement of cargo (figure 40) and parking lots.

d. TV controls should be enclosed in metal housing and properly secured to preclude attempted adjustment by unauthorized personnel. Delay caused by camera warmup and adjustment may be eliminated by keeping the camera in contiguous operation.

e. Normally, surveillance TV is of the low light level type (LLLTV) and can operate under marginal light conditions. A key consideration is maintenance of the TV system and supportive artificial lighting system.

7-28 Perimeter Intrusion Detection

The primary means of perimeter protection continues to be personal observation. However, such observation is usually limited to that performed by periodic patrols. Intrusion detection systems (IDS) may be valuable additional security aids if the perimeter requires continuous surveillance.

a. The decision to use IDS depends upon:

- Vulnerability and sensitivity of the protected area.
- Degree of protection necessary.
- Security aids currently in use.
- Availability of manpower.
- Cost effectiveness.

b. Usually, gates are protected by locks and intermittent patrol checks, or with security personnel on continuous duty. Intrusion detection systems at gates are not normally justified. However, if the gate is used only intermittently, or if additional protection is desired for the gate portion of the perimeter fence line, some system, such as a photoelectric system, may be used for this purpose.

Section IV
The Systems

7-29 Joint Service Interior Intrusion Detection System

The Joint Service Interior Intrusion Detection System (J-SIIDS) is a standardized set of intrusion detection system. components developed to provide physical security for interior areas. Protection of arms rooms was a prime concern in interior areas. Protection of arms rooms was also a prime concern in the development of J-SIIDS.

a. J-SIIDS has been **certified for use** in the following areas:

(1) Finance offices

(2) Post exchanges

(3) Class VI stores

(4) Narcotics storage areas

(5) Accountable property storage areas

(6) High value item storage areas

(7) CID evidence rooms

(8) Conventional weapons storage areas

(9) Billets and offices

(10) Aircraft hangars

(11) Nonconventional weapons and chemical weapons storage areas.

b. J-SIIDS is not certified for use in the following areas:

(1) Sensitive weapons storage areas (RED-EYE, DRAGON, LAW, and STINGER)

(2) Nuclear fuel storage areas

(3) Nuclear reactor facilities

(4) Computer centers

(5) Classified storage areas

(6) Areas where cryptographic devices are stored, used or maintained

(7) Ammunition and explosives storage and manufacturing areas

(8) Radioactive isotope storage areas

(9) Communication centers

c. This system consists of a family of sensors that can be used singly or in combination to provide detection of intrusion. Sensors are grouped into four categories-penetration, point, motion and duress. Signals from sensors are reported to the control unit (see figure 41), processed and transmitted to the monitor unit or audible alarm some distance from the protected area.

d. A J-SIIDS can be adapted for use in any arms room configuration by proper selection and installation to provide detection of unauthorized attempts to enter the protected area. A representative arms room installation is shown in figure 42 (next page).

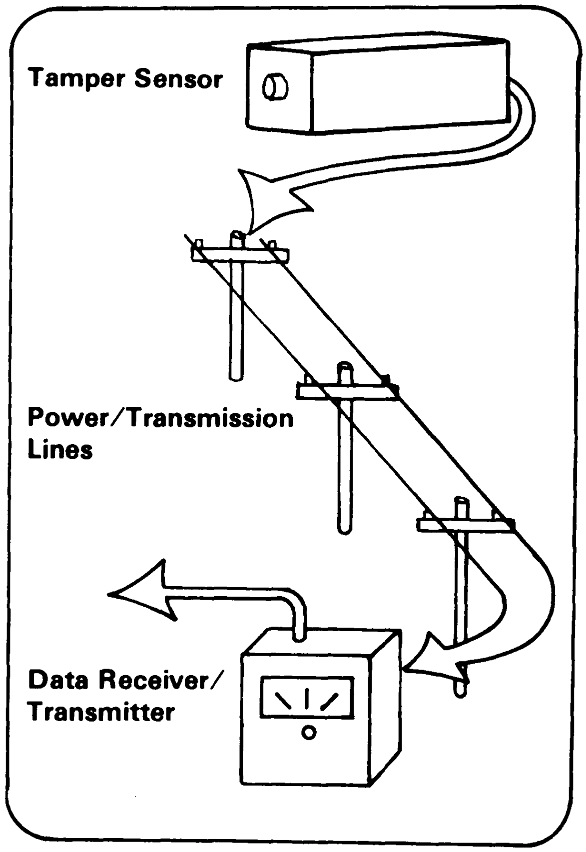


Figure 41—Control unit process.

e. The control unit for J-SIIDS is inside the protected area. It has tamper switches and dedicated telephone lines to carry a coded transmission to the monitor station. Any attempt to tamper with the telephone lines will cause an alarm.

7-30 J-SIIDS Component Categories

a. Sensors.

(1) Penetration sensors:

(a) Balanced magnetic switch
(b) Capacitance proximity sensor
(c) Grid wire sensor
(d) Vibration sensor
(e) Passive ultrasonic sensor

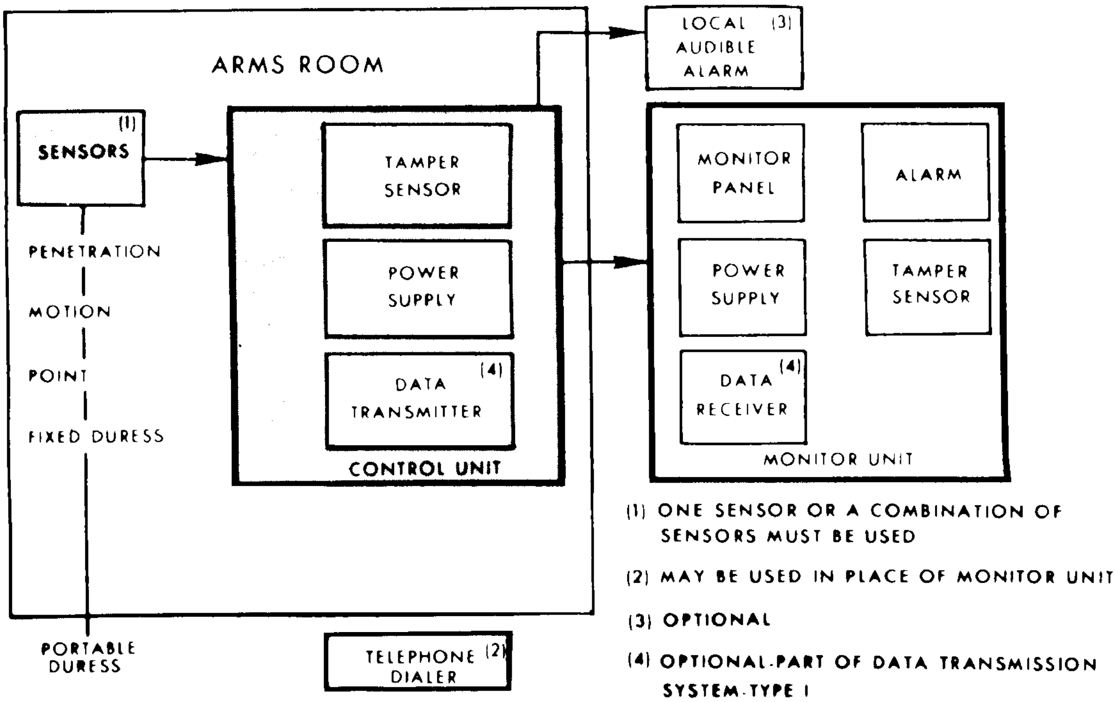


Figure 42—Example of arms room application of J-SIIDS.

(2) Motion sensor: Ultrasonic motion sensor.

(3) Point sensors:

(a) Magnetic weapons sensor
(b) capacitance proximity sensor

(4) Duress sensors:

(a) Fixed duress sensor
(b) Portable duress sensor.

b. Control unit.

c. Monitor unit.

d. Local audible alarm.

e. Telephone dialer.

f. Data transmission system (Type I).

g. The selection of components to make up each intrusion detection system depends on the physical characteristics of the specific area to be protected, operating characteristics of various systems, and the overall security program of the particular command or activity.

7-31 Addable J-SIIDS Components

a. Additional J-SIIDS components have materialized to provide more capabilities for protection of arms rooms and improve protection flexibility for areas other than arms rooms. In short, the components fill security voids in a basic J-SIIDS setup. Addable J-SIIDS components include:

- Commercial Alarm Monitor Interface (CAMI)
- Alarm Line Security Attachment (ALSA)
- Special Application Alarm Monitor System (SAAMS)
- Data Transmission System Resynchronization Kit (DTSRK).

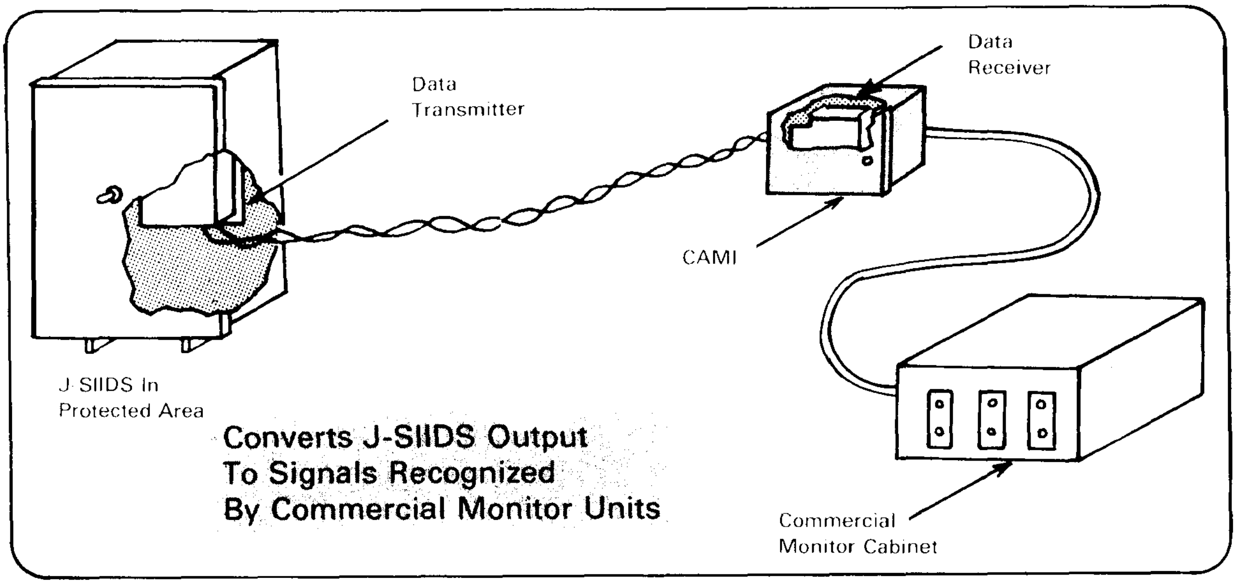


Figure 43—Commercial / J-SIIDS Alarm Monitor Interface (CAMI).

b. Commerical/J-SIIDS Alarm Monitor Interface (CAMI) (figure 43) will receive alarm-secure-access signals from an internal mounted J-SIIDS data receiver and electrically convert these signals to a format that will activate standard commercial alarm monitors. Many existing commercial alarm monitor stations are modular, allowing new modules to be plugged into a spare location in the monitor panel when additional protected areas are added to the system. For these areas, J-SIIDS can be monitored on the already available commercial type alarm monitor panel through the use of the CAMI rather than installing a J-SIIDS monitor unit.

c. Alarm Line Security Attachment (ALSA) (figure 44) consists of a printed circuit card mounted in the production J-SIIDS control unit and a complex terminating impedance mounted in each sensor signal processor enclosure. Circuitry on the card continuously monitors both the phase and amplitude of an a.c. signal on the alarm lines between the sensor signal processor and the control unit. If an attempt is made to inhibit a sensor alarm output by bridging across or

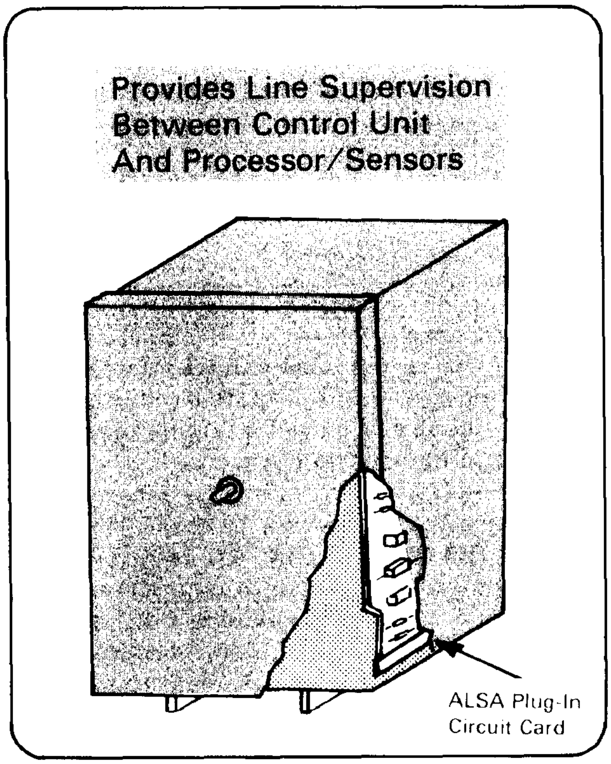


Figure 44—J-SIIDS Alarm Line Security Attachment (ALSA).

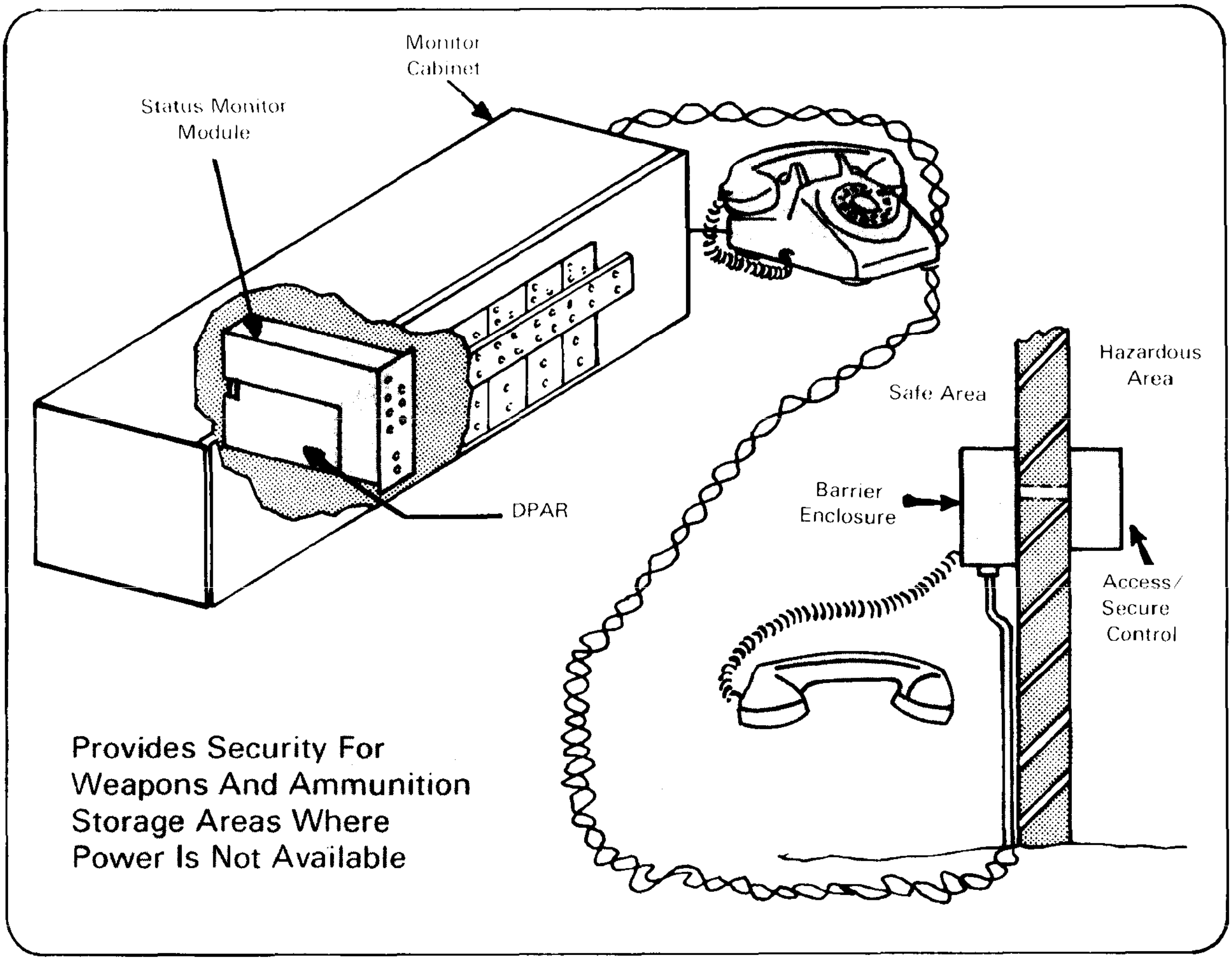


Figure 45—J-SIIDS Special Application Alarm Monitor System (SAAMS).

opening the sensor alarm lines, the ALSA will detect phase and amplitude changes in the a.c. signal and output a tamper alarm to the control unit alarm circuitry.

d. Special Application Alarm Monitor System (SAAMS) (figure 45) is an alarm monitor system designed to be intrinsically safe for use in Class I, Division I hazardous locations. The system uses nonpowered sensors, such as the J-SIIDS balanced magnetic switch and gridwire sensors, and interfaces with the J-SIIDS monitor cabinet. SAAMS consists of an access/secure enclosure (mounted inside the hazardous area), barrier enclosuere (mounted outside the hazardous area), a dual P annunciator receiver (DPAR) and a modified status monitor module which interface with the monitor cabinet, and a telephone circuit which allows voice communication between the hazardous area and the monitor site. The only voltages present in the SAAMS at the hazardous location are low level (less than 3 volts) a.c. signals placed on the transmission lines by the DPAR to monitor alarm and access/secure status of the hazardous location.

e. Data Transmission System Resynchronization Kit (DTSRK) (figure 46) is an electronic device designed to allow resynchronization of the J-SIIDS data transmission system from the monitor cabinet. This device

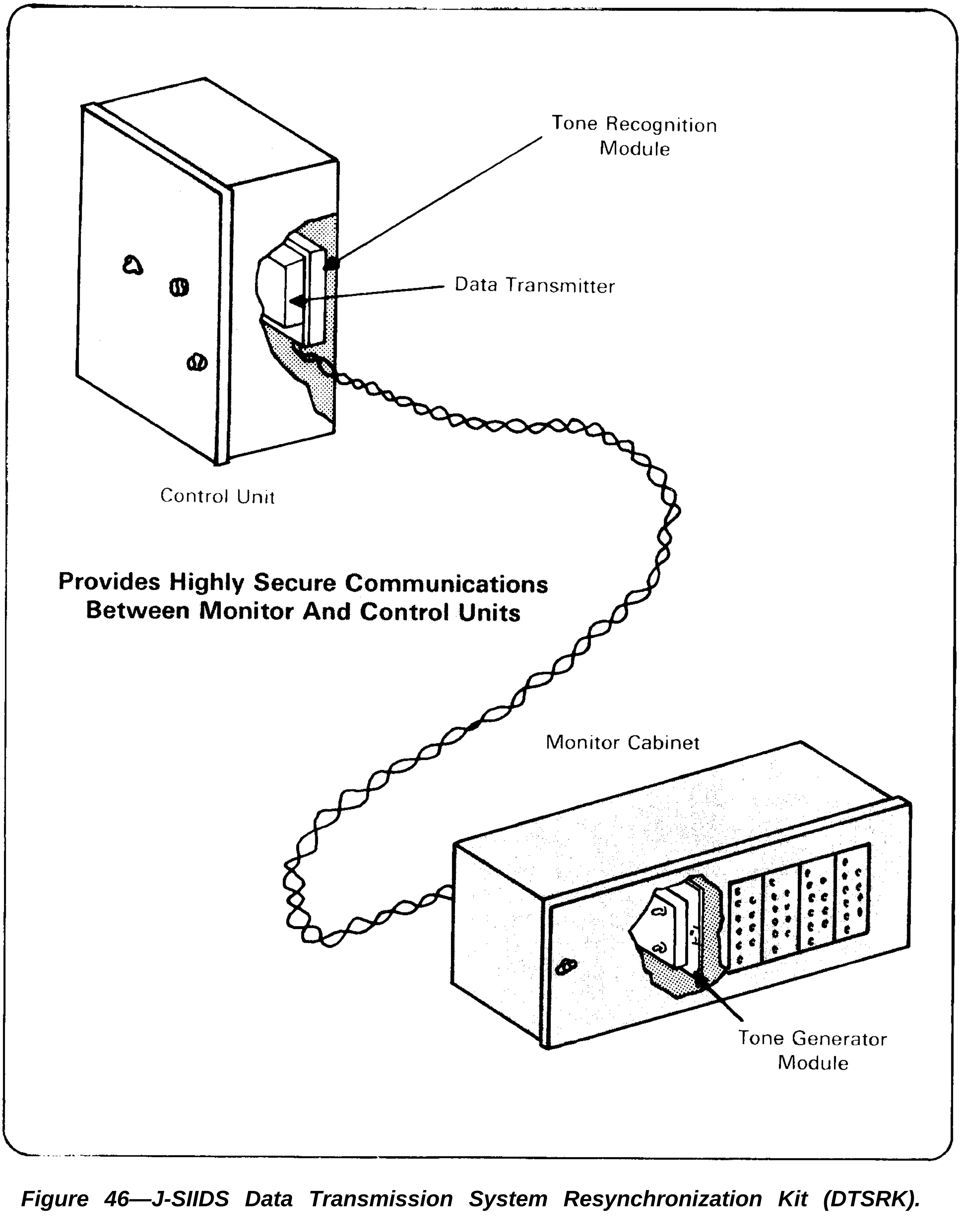


Figure 46—J-SIIDS Data Transmission System Resynchronization Kit (DTSRK).

will function over transmission lines up to 10 miles in length. The device consists of a tone generator module which interfaces with the monitor cabinet and a tone recognition module which interfaces with the control unit and data transmitter.

7-32 Facility Intrusion Detection System (FIDS)

FIDS (figure 47) is a joint service project, intended to provide DOD with a system to detect intrusions into, theft and pilferage from, or espionage/sabotage activities against all types of facilities worldwide. A valid requirement for FIDS exists because J-SIIDS did not meet the physical security requirement of the areas mentioned previously. FIDS is being developed for areas that presently are not protected by a standardized IDS.

a. Purposes:

(1) Developed for worldwide application containing improved communications, control, and display functions.

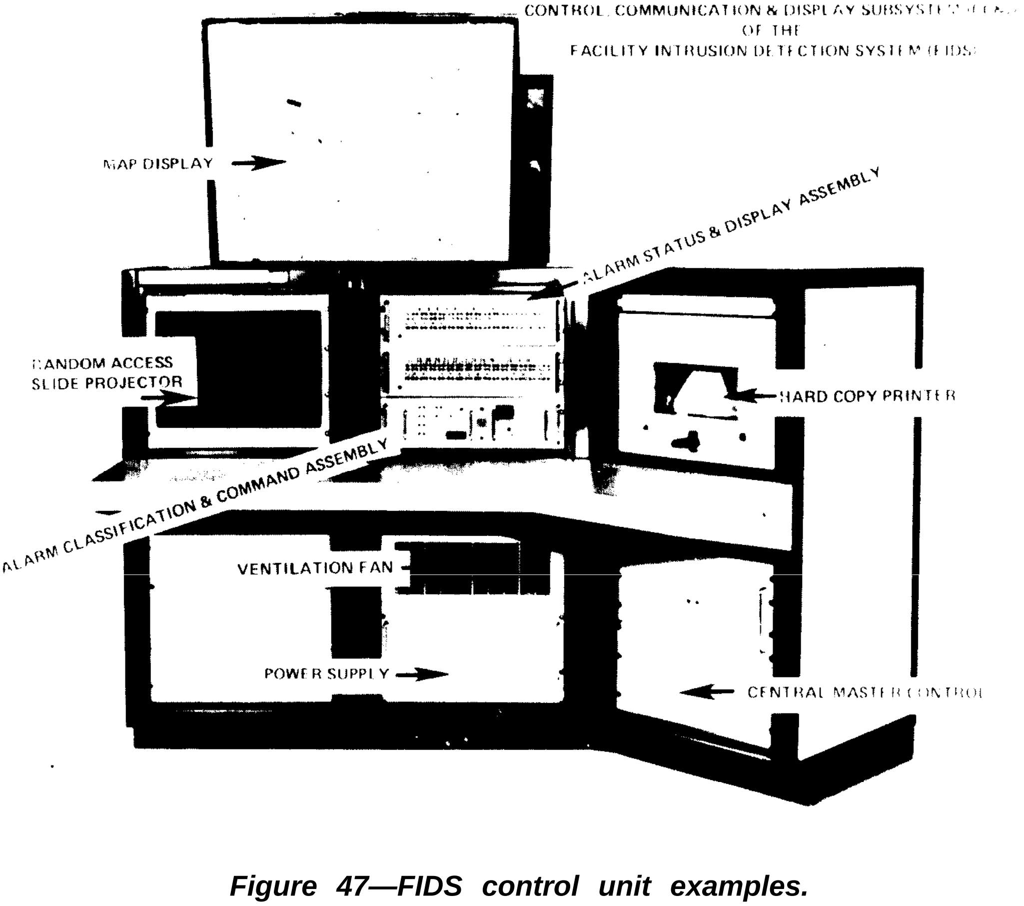


Figure 47—FIDS control unit examples.

(2) Provides an advanced additional detection and response capability that is not all inclusive with the J-SIIDS.

b. Additional capabilities:

- Worldwide operation
- Higher defeat resistance components
- Additional sensing capabilities
- Command capability
- Centralized processing and display capability
- Improved control unit and monitor unit
- Contraband sensors
- Entry control
- Improved duress sensors
- Response/deterrent system.

c. FIDS sensors come in four basic types, each with advanced characteristics. The four types are:

- Point
- Penetration
- Motion/Presence
- Duress.

(1) Basic characteristics for the point sensor involves capacitance proximity and magnetic weapon while the advanced characteristic concerns point contact strain only.

(2) Characteristics of the penetration sensor device in the basic configuration involves employment of:

- Vibration settings
- Grid wire
- Passive ultrasonic role
- Balanced magnetic switch(s).

The advanced stages of the penetration sensor involve point contact strain thermal and gamma effects.

(3) For the **motion/presence** sensor, its basic role concerns ultrasonic and large area motion. Advanced stages of the sensor concerns employment in a passive motion or a combination of ultrasonic/ microwave and ultrasonic/ infrared.

(4) Duress sensors' basic characteristic involves fixed duress situations and portable hand activated. It contains a physiological application in the advance stages.

d. FIDS' control, communications, and display system involves items, basic, and advanced uses as shown in fig. 48, page 120.

e. FIDS ancillary equipment has four characteristics—local alarm, entry control system, response force, and surveillance equipment.

(1) The local alarm in basic application involves an audible capability, while it displays a visual (flashing light) alarm signal in the advanced stage.

(2) In the basic stage, the entry control system uses keys, control card or pushbutton for entry application. In advanced application, the system uses:

- Fingerprint identification
- Voice analysis
- Handwriting analysis.

(3) The equipment's response device in the basic phase employs light activation, and is used in the advanced stage with:

- Electronic activated gates
- Recordings (warning, deterrent, etc.).

(4) FIDS ancillary equipment concerning

FIDS Control, Communications, and Display System

Items	Basic	Advanced
Control	Control Unit	
Data Transmission Link	Hardware (Interrogate/ Response)	Radio Frequency, Fibre Optics, and Strain Sensitive
Display System	Alarm and Status Display	
	Alarm, Classification, and Command Assembly	
	Hard Copy Printer	
	Map Display (Alarm Only)	
Power Supply (Backup)	Protected Area (d.c.)	
	Monitoring Area (d.c.)	

Figure 48.

surveillance capability identifies by audio in the basic stage, and identifies intruders through visual (CCTV) in the advanced stages.

f. FIDS is **certified for use in the following areas** (not for J-SIIDS application, par. 7-29b):

(1) Sensitive weapons storage areas (REDEYE, DRAGON, LAW, and STINGER)

(2) Nuclear fuel storage areas

(3) Nuclear reactor facilities

(4) Computer centers

(5) Classified storage areas

(6) Areas where cryptographic devices are stored, used, or maintained

(7) Ammunition and explosives storage and manufacturing areas

(8) Radioactive isotope storage areas

(9) Communication centers

(10) Nonconventional weapons storage areas and chemical weapons storage areas.

7-33 Fixed Installation Exterior Perimeter Sensor System (FIEPSS)

FIEPSS is a standardized security system to detect/prevent intrusion, forcible entry and/or unauthorized access into installations or facilities. This system consists of a family of sensors and a monitor unit. The sensors are classified as perimeter, barrier penetration, imaging, point, limited access, contraband, and duress. The system must be monitored from a central control.

a. Operational concept.

(1) The system must be deployed to detect the intrusion or attempted intrusion across installation perimeters, and boundaries of areas inside or outside the installation perimeter.

(2) It must also detect the unauthorized presence of personnel within the areas mentioned in the preceding paragraph and the unauthorized entry or removal of protected items within the area boundary.

(3) Security personnel in duress situations

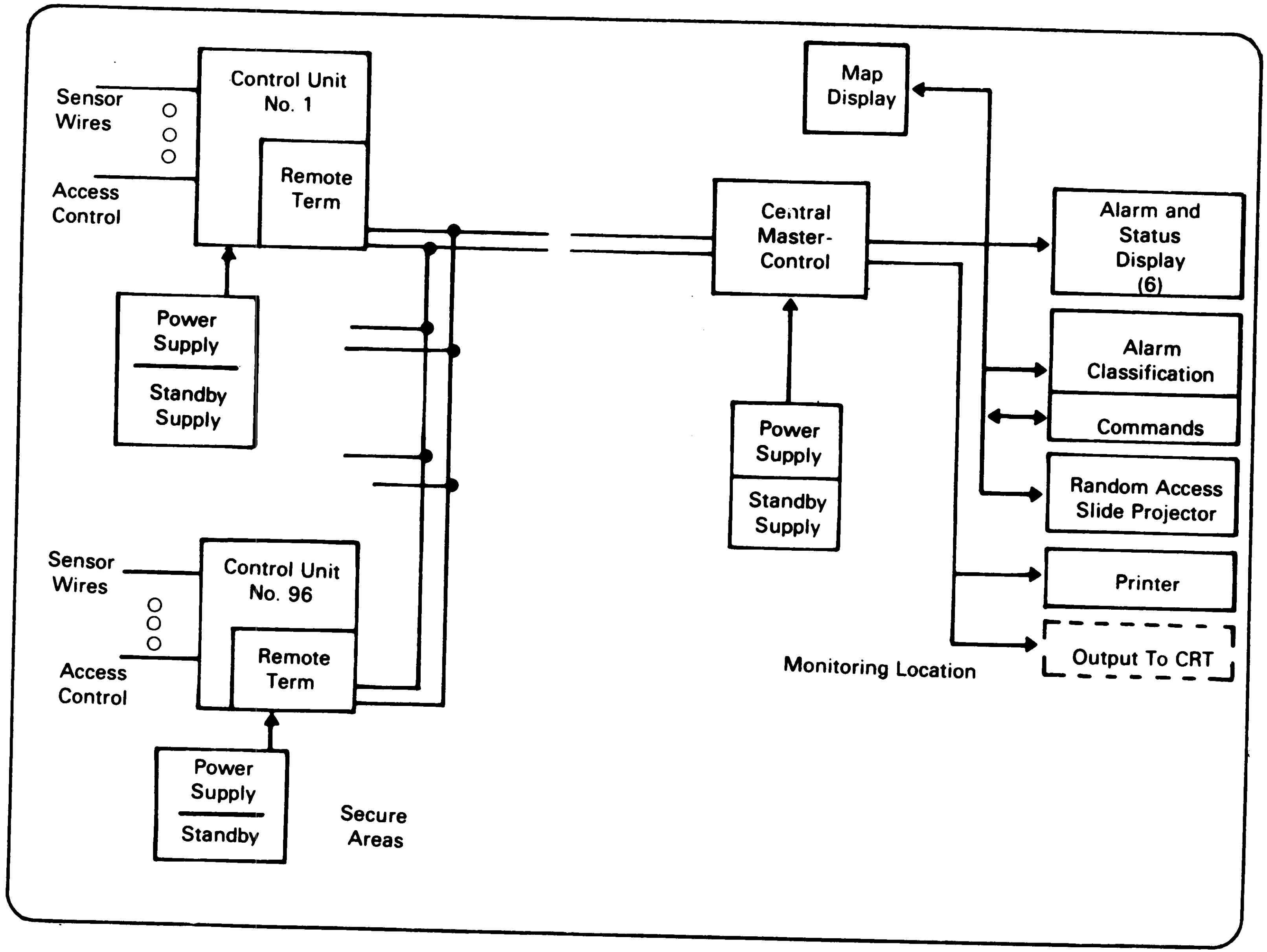


Figure 49—Example of FIDS component interface.

must be able, using this system, to activate a duress sensor to indicate a need for assistance.

(4) Each sensor component must be capable of announcing evidence of intrusion or unauthorized presence through a control unit to monitoring and display equipment located at the control center.

(5) The FIEPSS must provide the user flexibility and modularity in tailoring the system to the particular requirements of the installation and must be operated by installation security personnel.

(6) .Unmanned sensors will be employed along perimeters and/or around key facilities.

(7) A member of the security force must monitor the system in total and dispatch security forces to investigate alarms when activated.

b. Organizational concept. This system must be employed on an installation-by-installation basis in CONUS and OCONUS.

(1) Size and configuration of the system to be employed will be determined by the installation security manager.

(2) Some installations could employ a FIEPSS to completely cover its installation perimeters, while other installations might employ the system to cover an area within its perimeter, such as an ammunition storage area or a warehouse complex.

(3) Using units could vary from a total installation to selected units with special security requirements; such as ASA detachments. It is possible to have more than one FIEPSS on an installation.

c. Characteristics. The system will increase the mission reliability of personnel securing and protecting installation perimeters and areas of interest within and without the perimeter. It reduces losses due to pilferage, sabotage, espionage, organized ground attack, or other physical intrusion. The system includes following essential characteristics:

(1) Service and storage life of 10 years.

(2) Capable of operating continuously.

(3) Capable of being stored and operated in climatic categories 1-8, AR 70-38. The requirements of which can be met by means of a cold weather kit.

(4) Provide operation from primary and backup power sources. Backup power sources (batteries) must provide 24-hour minimum operation.

(5) Design consistent with electronic magnetic impulse (EMI) requirements of intended operational environments.

(6) Employed so that individuals cannot gain information by electromagnetic exploitation or other means that will enable them to defeat the system without an alarm being activated.

(7) Incorporate a self-test capability at the monitor unit to check functioning of the system.

(8) Capable of protecting several zones simultaneously.

(9) Consist of appropriate mixes of the following sensors:

(a) Perimeter sensors–Detect intrusion across or under a land boundary line to a minimum height or depth of five meters, or across or under a line on the surface of a body of water, which defines the perimeter of the area to be protected.

(b) Barrier penetration sensors-Sense intrusion or attempted intrusion through a physical barrier; such as a chain link fence, which is part of the perimeter of the area to be protected.

(c) Imaging sensor–Detect intrusion or

confirm the presence of an intruder announced by another type sensor.

(d) Point sensors—Detect someone approaching and/or touching a protected item; such as aircraft, vehicles, etc.

(e) Limited access/contraband sensors—Detect movement of persons or items into or out of the protected area.

(f) Duress sensors—Permit the stationary or roving guard force to signal for help in case of emergency.

(10) Have a control unit to provide primary power to sensors. The unit shall relay status of the sensor monitored area to the monitor unit. The system shall individually identify alarms from each sensor. Control unit shall monitor security of surveillance area by providing supervision of sensors, indication of change of power source and tampering or change of line integrity status. Unit shall automatically switch to self-contained emergency power should primary power supply fail. It shall provide the capability of simultaneous zone alarm in a guard tower as well as in the control center.

(11) Monitor unit displays the status and location of sensors by zone and/or sensor. Unit shall provide both audible and visual alarms, hard copy of all alarms and status changes and an output for a map display.

(12) Map display capability to indicate sensor locations with numbered light system keyed to a standard map or chart.

(13) Central console shall be capable of integrating data, providing display compatibility with the facility intrusion detection system and the remotely monitored battlefield area sensor system and commercial intrusion detection system and will include a map display capability.

(14) High probability (95-99%) of detection of skilled and semi-skilled intruders and organized forces.

(15) Data transmission system providing hard wire and/or RF data transmission capability between monitor and control unit. This system must provide for security of both hard wire and RF transmission, to include protection hardening of wire and encrypting of radio frequency (RF) transmission, if and when required. The system must provide the capability for initiating reactions, such as deterrent systems, lighting, imaging and listening devices, and responding to a systems test.

(16) Response unit to provide a command capability for illuminating an area and initiating deterrents, ranging from broadcast voice warning to application of force.

(17) Capability to identify and reject nuisance stimuli (false alarms) initiated by natural or manmade environments, either at the sensor or control unit, with a high degree of probability.

(18) Designed to have a specified mean-time-between-failure (MTBF) of 720 hours, assuming a system comprised of no more than 12 components. A failure of any of the 12 components is considered a system failure.

(19) Mean-time-to-repair (MTTR) for each subsystem shall not exceed 30 minutes for organizational maintenance and 60 minutes for DS and GS maintenance. Scheduled maintenance shall not exceed 2 hours for every 1000 hours of operation.

(20) Must to the maximum extent, be designed to modular replacement of reparir parts.

(21) Not susceptible to electromagnetic deception/countermeasures.

(22) Fail in the alarm mode for all faults.

(23) Safe to use at nuclear weapons storage installations.

(24) Designed to overcome these three

possible TEMPEST (compromising emanations) hazards:

(a) Flooding phenomena (as defined in NACSI 4000.3).

(b) Fortuitous conduction of compromising emanations from the facility being protected.

(c) Electromagnetic radiation of compromising emanations from the facility being protected.

(25) Designed for installation in accordance with Military Standardization Handbook (MIL HDBK) 232 whenever the facility being protected processes classified information electrically.

d. Data transmission system. Data transmission and display equipment being developed for J-SIIDS and Base and Installation security System (BISS) can be adapted to meet requirements of the basic system.

(1) The basic system consists of the following components:

(a) Control unit at installation perimeter to collect alarms from sensors and supply primary power to sensors.

(b) Hard wire/RF data transmission system from control unit to monitor unit.

(c) Monitor unit with status display modules.

(d) Status display map to be used with monitor unit when required.

(e) A buried line sensor for protecting land perimeters.

(f) A sensor for protecting perimeter fences.

(2) The complete system contains additional features such as:

(a) Central console equipment.

(b) A sensor for detecting penetration over or under water boundaries.

(c) A sensor for detecting human motion.

(d) Limited access/contraband sensors.

(e) Duress sensors.

(f) Response unit.

7-34 Base and Installation Security System (BISS)

BISS is a product of the US Air Force and is a standard for DOD. It has the capability of interfacing with other intrusion detection and sensor systems.

a. Functional role of BISS:

(1) Electronic surveillance
(2) Electronic detection
(3) Identification of intruders.

b. System description. The system being developed under this program consists of a wide variety of equipment and system segments, which when selected, configured and integrated for specific security situations will comprise electronic systems (such as, BISS) for particular situations.

(1) A single system configuration for all applications will not be the eventual product; but will be various types of equipment developed against a standard system specification. The important factor is that equipment can be integrated in various configurations and function

together as a system that will accept interior facility sensors (such as J-SIIDS and others).

(2) Such a system when employed provides a completely integrated electronic security system comprised of internal and external elements functioning under central command and control.

(3) The situations in which the BISS capability is applicable to worldwide are many and varied. These have been grouped into three categories (or modes of deployment) for system engineering-permanent installations, semipermanent installations (transportable mode) and mobile (quick reaction mode). Considerations in employing systems in these three distinctly different situations are varied, and are factors in engineering the BISS. However, they are factors which directly influence equipment and system segment engineering, and only indirectly the total system.

c. Application. Viewed from an operational application or functional standpoint, the initial system will consist of equipment in the following two subsystems.

(1) Detection is the basic subsystem for any system, and is comprised of sensors, and a sensor data transmission and display segment. Sensors that employ various techniques to detect the presence or movement of people and vehicles are being developed. Data transmission must be by hard wire with line security, and radio frequency (R/F). Either or both can be employed, depending on the situation.

(2) Surveillance uses various techniques to present on a remote monitor visual presentation of an area or location under surveillance. Surveillance may be for observing activity within a wide area, or assessing causes for sensor activations. (When a motion detection feature is incorporated, visual equipment can also be used as a sensor to signal movement.)

d. Intelligence. BISS is charged with developing enhanced intelligence capabilities for the security forces, enabling them to provide for physical security of DOD bases and installations.

(1) BISS will have application literally to every conceivable geographical location, operational environment, and external threat intensity. The common threat in defining the BISS threat model is, therefore, to be found in the operational concepts of its users. The shared threat for BISS is any individual, or group of individuals, who penetrate or attempt to penetrate a boundary, or who enter into an area of denied access. BISS provides detection, surveillance, and warning of such an intrusion, and, when possible, aids in response to an alarm stimulus.

(2) The operational response evoked from local security forces by the detection of intrusion must reflect the level of threat represented by the ingress depth of the intrusion. This reflected threat level depends on the existing external threat (hostile vs. nonhostile), ingress extent of the intrusion (area, boundary, or point), and the intrinsic value of the protected resource.

(3) In selecting the components of BISS, as well as in planning a specific BISS configuration, consideration must be given to both the nature of the threat and to the reflected level of the threat. (These are discussed more filly in following paragraphs.) When a user defines his BISS installation requirements, he must define his general threat level, including all possible escalations from that level. The user depends on his own intelligence channels to assist in his defining and maintaining the specific threat definitions associated with each of his specific configurations.

(a) Nature of threat. In general, BISS must function against both external and internal threats.

(b) Internal threats. Personnel who work in, or have intimate knowledge of the area and the security system are the source of internal threat. This threat is generally considered to be a human reliability problem. Susceptibility of this threat can be reduced by incorporating certain security measures and procedures into hard wire design, system installation and system operation. For example, boxes, sensor covers, and cables can be designed to make them less vulnerable to tampering; and communication networks can be provided with tamper detection capability through line supervision.

(c) External threat. The external threat can generally be divided into five categories—skilled, well-equipped, semi-skilled, organized force, and casual intruders.

■ Skilled and well-equipped intruder(s). These intruders would attempt penetrations to conduct military operations, espionage, sabotage and theft of sensitive or very high value items. They could be expected to plan their entry thoroughly and to carefully select the time and method of entry. Highly skilled intruders using professional, advanced techniques would probably attempt to covertly defeat or circumvent your intrusion detection and other physical protective measures. An intrusion detection system, however, can deter intrusion and can increase the difficulty of such an intrusion, resulting in a higher probability of detection.

■ Semi-skilled intruders. These intruders would attempt penetration to conduct terrorist or paramilitary activities, theft for profit, and/or vandalism. In addition, highly motivated and capable dissident groups or individuals may try to reduce confidence in the military establishment, embarrass the government, or create a dramatic incident to attract public attention. They would be expected to attempt entry without detailed planning or highly sophisticated equipment. They may evaluate the security posture by considering appropriate time factors, location vulnerability, and personnel/guard presence. They may attempt to bypass or otherwise defeat an intrusion detection system by covert means.

■ Organized force. Well organized units can be expected to use overt force and diversionary actions to gain entry. Efficiency, depth of planning, execution, and size of acting force may vary greatly. Altering intelligence will be necessary to upgrade the defense or security posture required to effectively counter this threat.

■ Casual intruders(s). These intruders would attempt penetration with little or no advance planning and without apparent rational purpose. They include thrill seekers and individuals who are mentally deranged or intoxicated. While they represent no military threat in the usual sense, it is possible they might inadvertently or with malicious intent cause considerable damage. An intrusion detection system should detect these intruders with very high confidence.

(d) Levels of threat. For convenience, the general levels of threat have been designated low, medium and high. The essential point is that each BISS configuration must take into account this general threat level and its possible escalations. BISS must contain a sufficient variety of modules to permit tailoring each configuration to meet its existing threat and yet provide the required interface capability to upgrade with minimum difficulty and expense in the event that the level of threat escalates. An **analysis of threat levels** is presented in figure 50. This figure also indicates appropriate levels of response by local security forces. Note that as the

Threat Level	Nature of Threat	Required Capabilities
Low	Stand off surveillance/espionage. Minimum/occasional penetration. Limited pilferage. Minor demonstrations.	Denial of surveillance and penetration. Detection and deterrence of intruders. Selective surveillance of critical areas. Deter intruders. Apprehension of pilferers.
Medium	All of low threat intensified. Sabotage. Harassment. Minor destruction and disablement. Dissident demonstrations.	Intensify response to low threat. Earlier detection. Immediate response (small groups). Increased mobility of response forces. Identification and location of sabotage. Capture of intruders.
High	All of medium threat intensified. Organized attack/armed conflict. Major destruction. Combat Intelligence.	Intensify response to medium threat. Complete penetration denial. Immediate response (large & small groups). Armed resistance, capture, destroy. Sabotage detection and prevention. Remote controlled and/or automated response capability. Interface with allied forces.

Figure 50—Threat analysis guidelines.

threat level escalates, requirements for probability of detection, reliability and degree of security required, as well as the speed and intensity of the local security response forces, also escalates.

7-35 Integration of Systems

When electronic protective systems are integrated there is great improvement in the overall security posture of an installation or activity.

A simple example of how DOD sensors would be integrated on an Army installation is shown in figure 51.

7-36 Remotely Monitored Battlefield Sensor System (REMBASS)

REMBASS, as an element of the sensor family, is used primarily in tactical situations in remote areas and acts as a squad or platoon early warning system.

a. REMBASS sensors.

(1) Target detection. Sensors must be able to detect personnel, vehicles, and aircraft (rotary wing only) using as few different technologies as possible.

(2) Target classification. Sensors must be able to classify the following:

Wheels	Tracks	Personnel
Heavy	Heavy	Armed
Light	Light	
(no bikes)		

(3) Sensor emplacement. Sensors must be emplaced by several different means, each offering its own operational advantages to the particular tactical operation. Methods of emplacement are hand, air, and ballistic. Sensors may be employed underground, on top of the ground, or in trees. Permanently or semipermanently emplaced line sensors to be used primarily for base defense are not considered part of REMBASS. However, base defense sensors which may be developed under other programs should be compatible with REMBASS readout elements.

(4) Disposition. Ballistically emplaced sensors must be expendable. Hand and air emplaced sensors must be retrievable during training and expendable during tactical operations.

(5) Emplacement accuracy. Emplacement accuracy is not a REMBASS requirement, but is the responsibility of the delivery platform or individual performing the emplacement. For target acquisition, this accuracy is critical; however, for general surveillance and early warning roles, less accuracy is required. Regardless, employment accuracies must be sufficient to accomplish the three REMBASS target classification roles. For surveillance and early warning, the emplacement accuracy of the individual or delivery platform is considered sufficient. Target acquisition sensors must have an emplacement accuracy sufficient to accomplish a 50-meter circular error probable for target location.

(6) Detection range. In general, sensors should have adjustable detection ranges. Maximum sensor detection ranges should not exceed:

(a) 100 m for personnel (single)X
(b) 1,000 m for vehicles
(c) 500 m for aircraft.

(7) Transmission range. All sensors must have an RF output capable of transmitting to an intended receiver (radio relay or readout unit) at a line-of-sight range of:

(a) 15 km ground-to-ground
(b) 100 km ground-to-air.

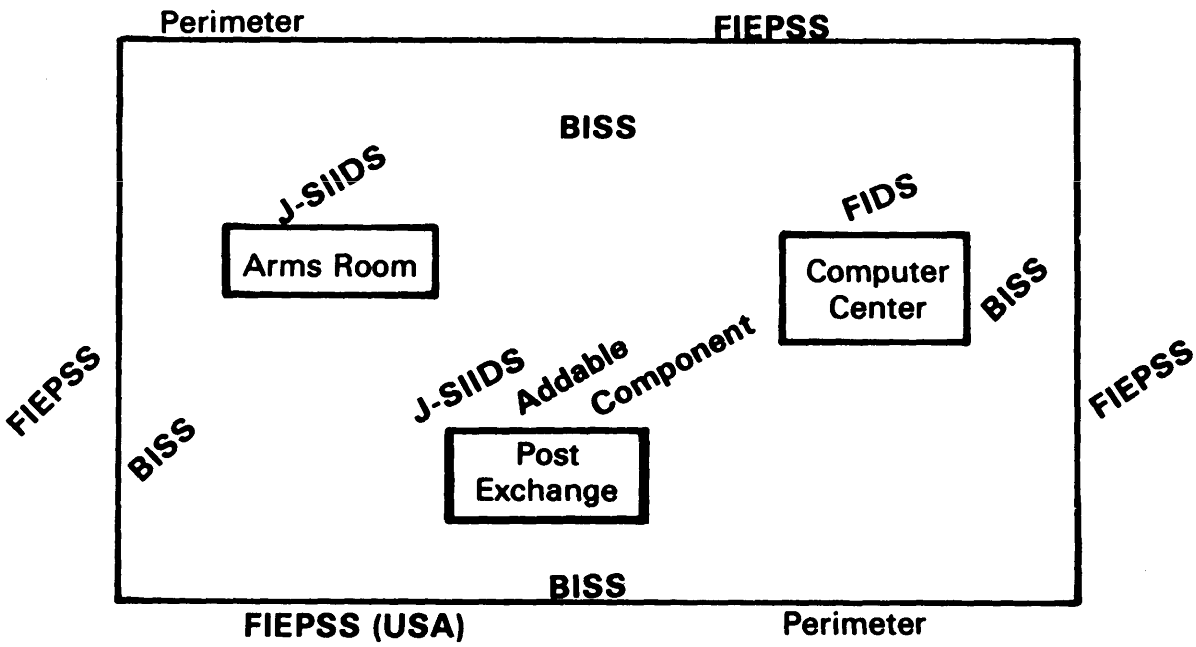


Figure 51—Simplifed example of an installation integrated protective system.

(8) Commendable features. A require ment exists for a commendable imaging sensor. Desired features are: on, off, trans- mit, and change viewing direction.

(9) Features required in all sensors:

(a) Selective mission duration (7, 15, or 30 days).

(b) Selective classification (if cost and operationally effective).

(c) Selective detection range sensitivity.

(d) Frequency and ID code that can be easily changed prior to mission.

(e) self-disable circuit to automatically activate upon end of programed life, malfunction, and/or tampering.

(10) Weight and size, including batter- ies. Hand emplaced sensors should be easily man-transportable. They should be less than 3 pounds and 100 cubic inches in size. Air emplaced sensors must be less than 20 pounds and 800 cubic inches. Ballistically emplaced sensors must be compatible in size and weight to the munitions for the anticipated delivery means.

(11) Mission life and reliability. All sensors must be capable of operating for 7 to 30 days. Strings of three or more sensors will have a 0.97 probability of successfully completing a 7-day mission.

(12) False alarm rate. Sensors will be designed so the system will experience an average false alarm rate per sensor of not more than 3 percent of alarms, or not more than one false alarm per 24-hour opera- tional period.

(13) Channel and ID selection. The capability to select frequency channel, and ID code by emplacement personnel in the field is required. Although such occur- rences are expected to be relatively infre- quent, the procedure and/or techniques to accomplish selection must be simplified.

(14) Realtime/nonrealtime outputs. Realtime outputs are desired for all sen- sors. Digital sensor alarms should be

realtime with an inhibit (update) time of 10 seconds. Since analog outputs from special acoustic and image sensors require much wider bandwidths, analog-to-digital conversion with delayed transmission times is acceptable, if the delay is not greater than 1 minute.

(15) Power supply. Each sensor requires an internal power supply that will function for the required mission duration in hot and cold environments. Hand emplaced sensors should have the capability to connect to an external alternating current (AC) or direct current (DC) power supply to extend mission life as much as 24 months.

b. Radio relays.

(1) Types. The depth of sensor emplacements in the division area of interest requires a variety of emplacement techniques for relays (hand, air, and ballistic). If size and cost constraints permit, each relay should be capable of transmitting the digital sensor and command signals as well as the signals from imaging or acoustic sensors. Hand emplaced relays must be capable of operating from the ground, from a vehicle, or in an aircraft (without requiring a dedicated vehicle or aircraft).

(2) Channel selection. Selections of desired channels or desired frequency bands for relays may be required in the field by emplacement teams. If narrow band frequency shift keying (FSK) is used for a data transmission system, each type of relay will require a dual channel capability .

(3) Disposition. All relays must be expendable during armed conflict. In peacetime, relays must be recovered and used to the maximum extent.

(4) Transmission range. All relays must have an RF output capable of extending each transmission link by 15 km. That is, the relay must be able to transmit to an intended receiver at a line-of-sight range of 15 km ground-to-ground. Airborne relays must have a line-of-sight range of 100 km.

(5) Storing and time tagging. Each relay, with the addition of an attached module, must be capable of storing and time tagging activity and providing this data upon command.

(6) Self-disable features. These features, which must automatically activate upon end of programed life, malfunction, tampering, and/or end of battery life, should be included in all relays.

(7) Size and weight. Hand and air emplaced relays should not exceed 1.5 cubic feet and 30 pounds. Ballistically emplaced relays must conform in size and weight to the munitions for the anticipated delivery means.

(8) Mission life and reliability. All relays must be capable of operating for a 1 percent duty cycle for up to 30 days on internal power sources. The reliability of three relays in a series must equal 0.87 for a 7-day mission.

(9) Power supply. All air and ballistically emplaced relays require internal battery supplies. Hand emplaced relays should have provisions for external power supplies. Airborne relays require provisions for using aircraft power.

(10) Storage capability. To retransmit near realtime audio or image information, a store and forward feature may be required.

c. Basic readout unit.

(1) The readout unit must be the basic sensor monitoring device in the REMBASS. The readout unit must consist of a receiver, hard copy printer or chart record, and a backup visual display.

(2) Input/output features. Readout input will be RF from the sensors or relays. The primary output from the readout should be hard copy. A visual light display

backup is also necessary. Output should provide the following information:

(a) Sensor identification
(b) Type target (classification)
(c) Timing information.

Auxiliary outputs must be provided for image and acoustic processing devices.

(3) Frequency selection. Manual selections of frequency channels will be necessary. There is a requirement for a dual channel receiver in the basic readout unit for limited electronic warfare (EW) protection and for monitoring flexibility.

(4) Power requirements. Readout devices require an internal battery and external AC/DC power capability. The readout must function continuously for 15 hours without requiring battery change.

(5) Computing requirements. When fewer than three readouts are collocated, limited computing capability is required. This may involve a simple nomogram or a small electronic calculator. The sole purpose of the nomogram or calculator is to assist the operator in determining REMBASS functions.

(6) Weight and size. The readout should be man-portable, weigh less than 8 pounds, and be no more than 0.5 cubic feet in volume.

(7) Reliability. Readout reliability must equal 0.94.

d. Command transmitter.

(1) The command transmitter must provide signals to the commendable relay. It must be separate from the readout unit so each can be employed independently.

(2) Power requirements. The command transmitter should have an internal battery and an external AC/DC power capability. It must function. for a 7-day mission without requiring battery change.

(3) Transmission range. A command transmitter must be capable of transmitting over a line-of-sight path of 30 km to either a relay or sensor.

(4) Command outputs. A command transmitter must be capable of addressing commendable sensors and relays on appropriate frequencies and with appropriate ID codes. (In-band command is preferred.)

(5) Weight and size. The command transmitter should be man-portable, weigh no more than 4 pounds, and not exceed 0.4 cubic feet in volume.

(6) Reliability. The command transmitter must have a 0.80 probability of successfully completing a 7-day mission.

e. Special processing unit.

(1) The special processing unit must provide a processing and computing termination for three or more basic readout units. This is a nonessential device used to expand and facilitate operator functions when readout units are stacked within the monitoring site. Sensor activation information from the readouts would be processed so that the printout from the special processing unit will provide:

(a) Sensor activation by ID and time.
(b) Target classification.
(c) Target location in universal transverse mercator grid coordinates.
(d) Direction of movement.
(e) Speed.

(2) Inputs. The processing unit must provide with minimal human interface the same computational capability required of the nomogram or calculator used with a single readout unit. The processing unit must receive inputs from one to six readout units. These units should be either plugged or cabled to the processing unit.

(3) Outputs. The primary output for sensor information would be page print. There may be a need for a paper tape or ADP link which can conveniently interface with the integrated battlefield control

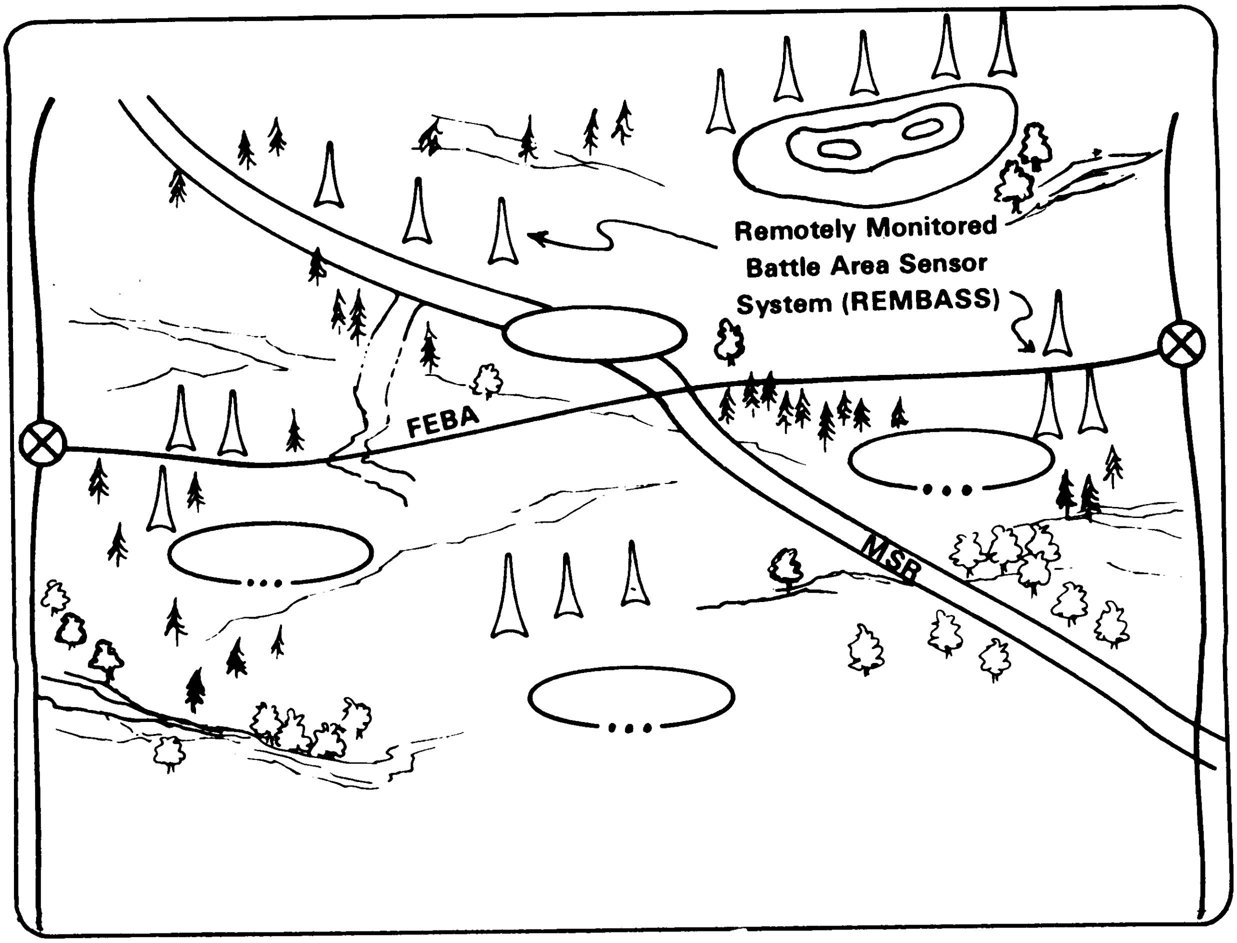


Figure 52—Example of REMBASS tactical employment.

system (IBCS) or tactical operations svstem. This need cannot be established until the IBCS concept is defined explicitly. Auxiliary imaging and audio display/ monitors can be attached to the processing unit for special applications.

(4) Power requirement. The special processing unit should not require internal battery power. An external AC/DC power capability must be provided. The special processing unit should be capable of operating from aircraft and vehicular sources, tactical generators, and external commercial AC sources.

(5) Weight and size. The processing unit should weigh no more than 30 pounds and should not exceed 1.0 cubic feet in volume.

(6) Reliability. The special processing unit must have a 0.948 probability y of successfully completing a 7-day mission.

7-37 Intrusion Detection System for Nuclear Storage (AR 50-5)

a. The **basic electronic security system** must consist of an interior sensor integrated by data transmission links into the annunciator console.

(1) All nuclear weapons storage structures at permanent sites must be protected by primary intrusion detection systems. Alternate backup systems, operated on a different principle of detection, and remote annunciator panels are desirable.

(2) Systems must provide both audible and visual alarm indications and must be dependable, easy to maintain in their operational environment, and adequately protected against tampering. They must give an alarm in case of failure, have low nuisance-alarm rates, and be equipped with a protected, prompt, online alternate source of power or an emergency battery power source.

(3) Systems must be installed and designed so that all portions of the system, including data transmission lines, are protected against tampering.

(4) At sites supporting Allied units, some additional monitor equipment may be required to facilitate US and user-nation coordination.

(5) If the telephone communications system is owned by the Government and maintained and operated by military or civilian employees who have suitable security clearances, wires in the cables may be used for intrusion detection circuits. Otherwise, detection circuits must not be earned in cables that also contain telephone or other electrical circuitry.

b. Interior sensor equipment. As a minimum, protection must be provided to detect entry into a storage structure or maintenance facility used for overnight storage.

c. Control/data transmission (communications).

(1) Hard wire data transmission links must be used for interior sensor components. All transmission lines for alarm circuit should be completely contained in a secured area and must be adequately safeguarded to preclude tampering. If the transmission lines must leave the secured area, they must be inspected frequently by guards. A line supervision system should be installed to monitor lines connecting the intrusion detection devices to the monitor panel. Supervision may be accomplished by monitoring various modes/deviations/random line signals (such as digital, tone, frequency encoding, and others) and must at least equal the following acceptable mode and supervisory criteria, activating an alarm signal when any of these criteria are exceeded:

(a) As much as 5-percent change in normal line signal, if it consists of direct current from 0.5 milliampere through 30 milliamperes.

(b) As much as 10-percent change in normal line signal, if it consists of direct current from 10 microampere to 0.5 milliampere.

(c) As much as 5-percent change in any component of the normal line signal, if it consists of an alternating current of a frequency from 1 through 100 Hz and 0.5 milliampere through 30 milliamperes.

(d) As much as 15-percent change in any component of the normal line signal, if it consists of an alternating current of a frequency of higher than 100 Hz superimposed on a direct current that has any value from 0.5 milliampere through 30 milliamperes.

(2) Alarm circuits with a remote test capability must be tested at least once during each guard relief. When a remote test is not possible, circuit tests must be conducted at least once every 24 hours by activating detection devices. Inspections must be made at least semiannually by maintenance personnel qualified to repair or replace worn or failing components and to detect evidence or indications of tampering with any portion of the system.

(3) Prior to maintenance or repair, the system must be tested, as in (2) above, and a record made of each sensor/alarm

operating status. The monitoring operator must deactivate only that portion of the system to be repaired and continue to monitor the balance of the system. Immediately after completion of repair or maintenance, the entire system must be tested again, as in (2) above. In addition, those circuits on which repair or maintenance was performed must be tested by physically activating the detection devices.

d. Records. Commanders must insure that personnel monitoring primary annunciator panels maintain records of the data listed in (1) through (9) below. These records, retained for 1 year, will be used for evaluating intrusion detection system effectiveness (including reliability, sensitivity, required adjustments or maintenance, and other information intended to maintain or increase security):

(1) Date, time, and prevailing weather conditions when an alarm signal is received.

(2) Identity of the guard recording the alarm.

(3) Identity of the area from which the alarm was activated.

(4) Cause of the alarm.

(5) Action taken in response to the alarm.

(6) Total elapsed time required by responding personnel to reach the scene.

(7) Tests of detection circuits.

(8) Malfunctions.

(9) Servicing and/or maintenance of the systems .

7-38 Intrusion Detection System for Arms Rooms (AR 190-11)

a. All structures designated for permanent storage of firearms except as specified in AR 190-11, must be protected with an intrusion detection system or be under surveillance by a guard, closed circuit television, or onduty personnel. The IDS used must contain a duress signaling component. Alarms must be annunciated at a location from which a designated response force can be immediately dispatched. Alarm signaling with only a local audible alarm is unauthorized.

b. As a minimum, IDS installed for protection of arms rooms must consist of two types of sensors with different methods of activation (such as a balanced magnetic switch on the doors and ultrasonic motion sensors inside the arms room). Additional levels of protection, where practical, are encouraged. In selecting the mode of operation desired for each arms room, it should be emphasized that an interior IDS is designed to detect, not prevent, an intrusion. Therefore, a comprehensive physical security plan must contain appropriate physical security measures and procedures for an effective reaction force. To insure this, IDS must be installed so that alarm signals can only be cleared by entering the protected area. Remote clearing of alarms prior to entering and checking the alarm is not authorized.

c. The Joint Services Interior Intrusion Detection System (J-SIIDS) will be used as the initial IDS or as replacement for installed commercial systems at onpost facilities. Installation of J-SIIDS at offpost facilities is optional depending upon cost effectiveness, ease of maintenance, and monitoring. Commercial IDS are authorized for installation in facilities off post where J-SIIDS is not employed.

d. Installers and maintainers of the J-SIIDS must have as a minimum, a favorable national agency check or foreign country equivalent prior to having access to J-SIIDS. This includes military personnel, DAC, foreign national employees, civilian contractors or contract foreign nationals. A current list of cleared installer/maintenance personnel must be maintained by the facility

engineer. The **key to access test/retest switch** must be maintained and only those persons on the arms room key roster will be authorized access to these keys on a need to have basis. Keys to the control unit door and monitor must be secured separately from the access test/retest keys, and only authorized maintenance men, whose identity has been verified at the direction of the unit/activity commander, will be authorized access to these keys. Commanders must insure unit personnel will not have access to the interior of the control unit or monitor. All keys to J-SIIDS or commercial equipment must be under control of the commander whose storage area is being protected. Keys must be secured in containers as required for arms room keys; however, they must not be retained together with arms room keys. Wiring diagrams or other instructions developed by the installer to assist maintenance personnel must be stored inside the control unit door in the space provided. Such documents must be marked FOR OFFICIAL USE ONLY (FOUO).

e. When intrusion detection systems are used at arms storage rooms in civilian communities, arrangements must be made to connect alarms to local civilian police agencies, campus police headquarters, or private security companies. There must be a designated response force that can be immediately directed to respond in case of an alarm from the protected area.

f. A daily log must be maintained by monitor stations of all alarms received from arms/ammo storage facilities. The log must indicate, as a minimum: time, date, and location of alarm; identity of individual receiving alarm; nature of cause of the alarm; and action taken in response to the alarm. The logs must be maintained for 3 months. Problem areas identified must be brought to the attention of the troop support command.

g. Transmission lines from control units to monitor panels that are open or accessible to tampering must be electrically supervised. As a minimum, a 24-hour backup power source most be provided for each control unit and monitor panel.

h. Commercial IDS equipment is authorized when J-SIIDS is not available or considered impractical. When government type-classified systems are to be employed, the applicable installation manual must be used. Plans and specifications for installation of commercial IDS equipment must be forwarded through command channels to the Chief of Engineers, HQDA (DAEN-MCE-D), WASH, DC 20314 for final technical review and approval.

i. Periodic systems operational checks must be made and logged by unit security personnel, to include visual inspection of components and conduit for evidence of tampering, operational checks of sonsors to insure stimuli activate the sensor.

j. Installation physical security inspectors should include a check of each IDS during any announced security inspections. Checks should include visual inspection of components and conduit for evidence of tampering, operational checks of the system in accordance with procedures outlined in section V, chapter 5, TM 5-6350-262-14/14 under abbreviated system check test. This same test can be modified and applied to any commercial system. Checks should also be made of unit log entries and records regarding operation and inspection of IDS.

7-39 Maintenance of IDS

a. Intrusion detection systems should remain in **continuous operation** during nonoperational hours of the protected activity if they are to be effective security aids. In some situations it may be necessary to have continuous 24-hour operation. Therefore, preventive and corrective maintenance should be performed properly. Each system should be capable of operating from a standby power source to compensate for the vulnerability of power sources outside the

installation. The time requirement for such capability must be evaluated in each case dependent upon such factors as alternate power supplies, maintenance support, hours of active operation, and so forth.

b. Maintenance is not a difficult problem if proper care is routinely exercised. Most malfunctions, if the system has been properly selected, installed, and adjusted, result from improper maintenance. To prevent malfunctions, all component parts must be regularly inspected and tested by qualified personnel as often as recommended by manufacturers. Spare parts, such as fuses, condensers, relays, and other parts as recommended by the manufacturer, should be stocked locally.

c. Normally, the manufacturer will train and advise personnel on maintenance of their equipment. To insure proper operation of detection systems, the following should be observed.

(1) Designated unit personnel should be available and capable of effecting immediate minor repairs, to include replacement of burned out bulbs, replacement of fuses, maintenance and replacement of the auxiliary power unit, and correction of obvious causes of malfunctions and invalid alarms. All other forms of replacement parts and repairs should be provided by support maintenance personnel.

(2) If an installation cannot furnish support maintenance personnel, a service contract should be negotiated with the manufacturer. In either case, maintenance service must be available on a 24-hour basis. Maintenance response time to critical areas should be no more than 3 hours.

d. Operating and maintenance personnel should be cleared for access to classified information to the degree necessary for access to the area concerned. Plans and diagrams showing location and technical data of installed systems, signal transmission lines, and monitor units should be classified and protected accordingly.

e. The alarm receiving area should be designed to give adequate protection to monitor personnel, as this will be a prime target for intruders. Provision for emergency assistance to this area should be established. Appropriate measures should be employed to insure that monitor personnel maintain the system's integrity. Admittance to this area should be restricted to supervisory and maintenance personnel.

f. Personnel on duty at monitor units at installations or facilities using intrusion detection systems should maintain a daily record of all systems including the number of alarms and any malfunctions experienced. Operational records should reflect the following:

(1) Date, time, and prevailing weather conditions.

(2) Identity of person recording alarm signal.

(3) Identity of area from which alarm signal is received.

(4) Action taken in response to alarm signal received.

(5) Total time required by responding personnel to arrive at the scene of an alarm.

(6) Cause for alarm signal to be activated.

(7) Tests of alarms.

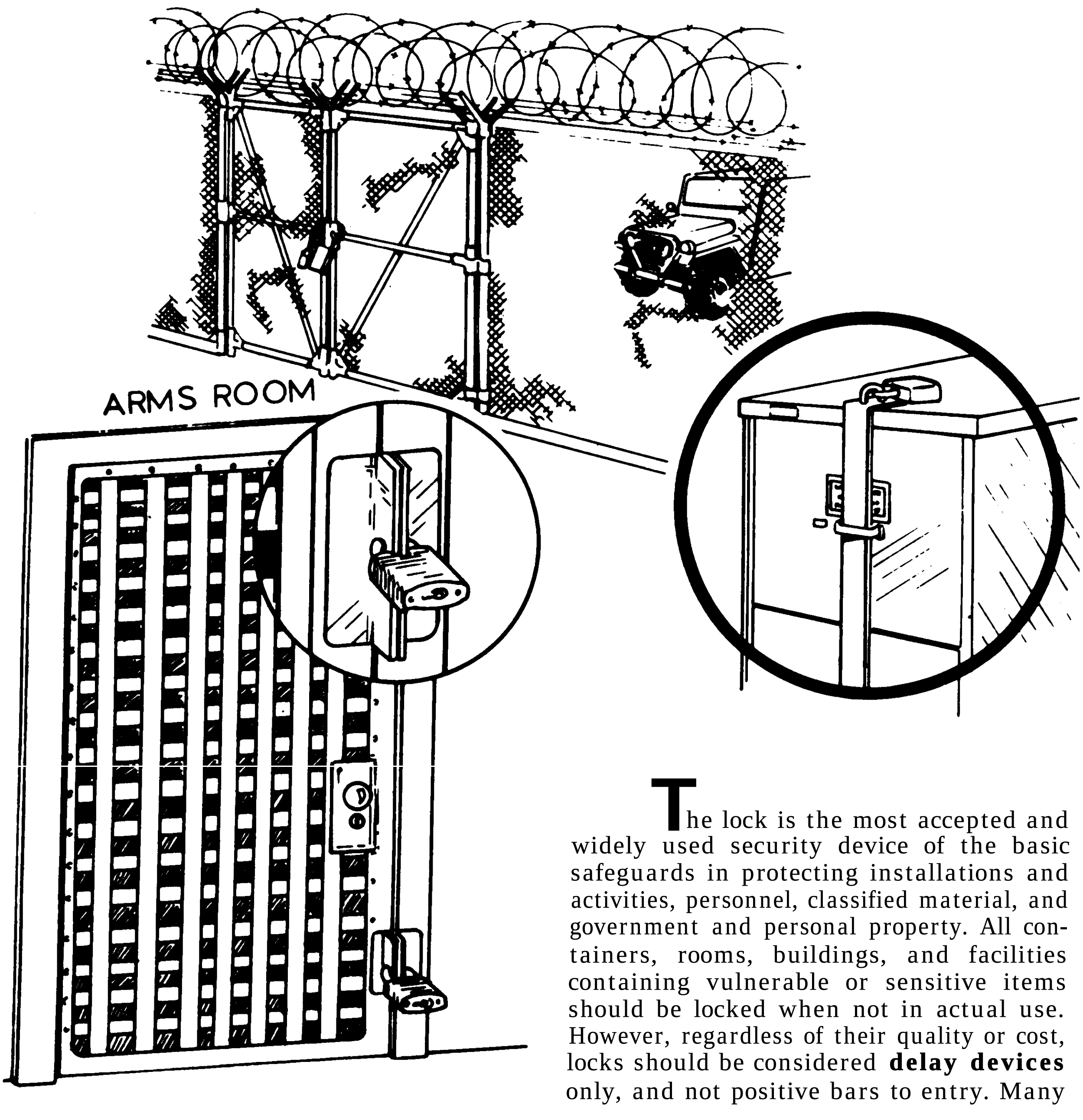
(8) Malfunctions, including nuisance alarms.

(9) Servicing/maintenance of detection systems.

g. Maintenance for the J-SIIDS, J-SIIDS addable components, FIEPSS, FIDS, and BISS must be in accordance with the technical manuals published in support of the equipment.

Chapter 8

Lock and Key Systems



The lock is the most accepted and widely used security device of the basic safeguards in protecting installations and activities, personnel, classified material, and government and personal property. All containers, rooms, buildings, and facilities containing vulnerable or sensitive items should be locked when not in actual use. However, regardless of their quality or cost, locks should be considered **delay devices** only, and not positive bars to entry. Many

153-846 0 - 94 - 8

ingenious locks have been devised, but equally ingenious means have been developed to open them surreptitiously. Some types of locks require considerable time and expert manipulation for covert opening, but all will succumb to force and the proper tools. Therefore, the locking system must be backed up with other security measures.

8-1 Installation And Maintenance

a. The Army Corps of Engineers is responsible for installation and maintenance of locks, latches, padlocks, or other locking devices on doors, cabinets, vaults, and similar built-in items that are an integral part of a building or structure. Locks and locking devices are listed by manufacturer and catalog number in TM 5-805-8. Conversely, locking devices for safes, lockers, cabinets, desks, and similar items that are not an integral part of a building are not the responsibility of the Army Corps of Engineers (AR 420-70).

b. Certain Army regulations (such as 190-11, 50-5, 50-6) prescribe specific types of locks for specific types of installations or facilities, and provide the National Stock Number (NSN) in each case. AR 380-5 prescribes standard facilities for storage of classified material.

8-2 Types of Locking Devices

The degree of protection afforded by any well-constructed vault, safe, or filing cabinet may be measured in terms of the resistance of the locking mechanism to picking, manipulation, or drilling. Types of locking devices include:

(1) Key locks. Most key locks can be picked by an expert in a few minutes. The possibility of the loss and compromise of a key and the possibility of an impression being made should also be considered in determining the security value of a key-type lock.

(2) Conventional combination locks. This type lock may be opened by a skillful manipulator, who may be able to determine the settings of the tumblers and construction of a common three-position dial-type combination lock through his sense of touch and hearing. Although the manipulation of some combination locks may require several hours, a skillful manipulator can open an average con ventional combination lock in a few minutes.

(3) Manipulation-resistant combination locks. A manipulation-proof lock is designed so that the opening lever does not come in contact with the tumblers until the combination has been set. Such a lock furnishes a high degree of protection for highly-classified or important material.

(4) Other combination locks. Combination locks with four or more tumblers may be desirable for containers of highly important items.

(5) Relocking devices. A relocking device on a safe or vault door furnishes an added degree of security against forcible entry. Such a device appreciably increases the difficulty of opening a combination lock container by punching, drilling, or blocking the lock or its parts, and is recommended for heavy safes and vaults.

(6) Interchangeable cores. The interchangeable core system uses a lock with a core that can be removed and replaced by another core using a different key. Its main features include:

(a) Cores may be quickly replaced, instantly changing the matching of locks and keys if their security is compromised.

(b) All locks can be keyed into an overall complete locking system.

(c) Economical due to reduction in maintenance costs and new lock expense.

(d) System is flexible and can be

engineered to the installation's needs.

(e) Simplifies recordkeeping.

(7) Cypher locks. A cypher lock is a digital (pushbuttons numbered from 1 through 9) combination door locking device used to deny area access to any individual not authorized or cleared for a specific area.

8-3 Understanding Lock Security

a. Combination locks— This popular type of lock is incorporated in padlocks, vaults, and doorlocks. The operation principle of most combination locks is a simple one. The operator uses numbers (or other symbols) as reference points to enable him to aline tumblers so that the locking parts of the lock can move to an unlocked position.

(1) Figure 53 represents a three-tumbler combination lock mechanism. (A combination lock has the same number tumblers as there are numbers in the combination. Therefore, a lock having three numbers in the combination has three tumblers; four numbers, four tumblers, etc.) In figure 53 "A" represents the dial, which is firmly fixed to the shaft "E". Any movement of the dial is directly imparted to the shaft. Letters "B," "C," and "D," identify the tumblers.

Each tumbler resembles a disc with a notch cut into its circumference. This notch is called a gate. "D" represents the driver tumbler. It, like the dial, is firmly fixed to the shaft so that when the dial is moved, the driver tumbler also moves. "B" and "C" are called rider tumblers. They merely rotate around the shaft. Therefore, movement of the dial may not immediately impart corresponding movement to the rider tumblers.

To operate the lock, one must aline the gates with the fence; when the fence is free

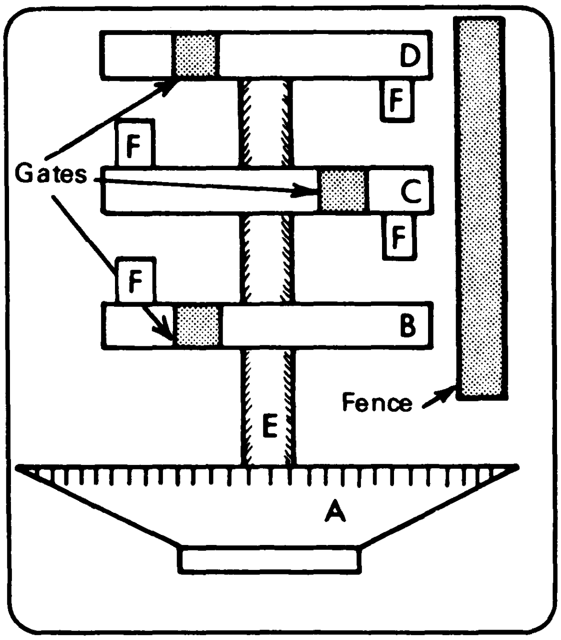


Figure 53—How a three-tumbler combination lock works.

to move into the space made by the gates, the lock will operate. First, the dial is rotated in one direction several times. The driver follows the dial and within a 360-degree turn, the drive pin "F" on the driver comes into contact with the drive pin on rider "C" causing "C" to rotate in the same direction. As the dial continues to turn in the same direction, the drive pin on "C" contacts the drive pin on "B" and then all the tumblers are nested (that is, all tumblers are going in the same direction).

The operator then stops the dial when the first number of the combination comes into alinement with the index mark on the front of the lock. This will aline the gate on tumbler "B" with the fence. He then reverses direction and rotates the dial one less turn to the next number of the combination. This allows "B" to remain in alinement while "C" comes into alinement. Changing direction and turning the dial one less turn again brings "D" into alinement and the lock will now open.

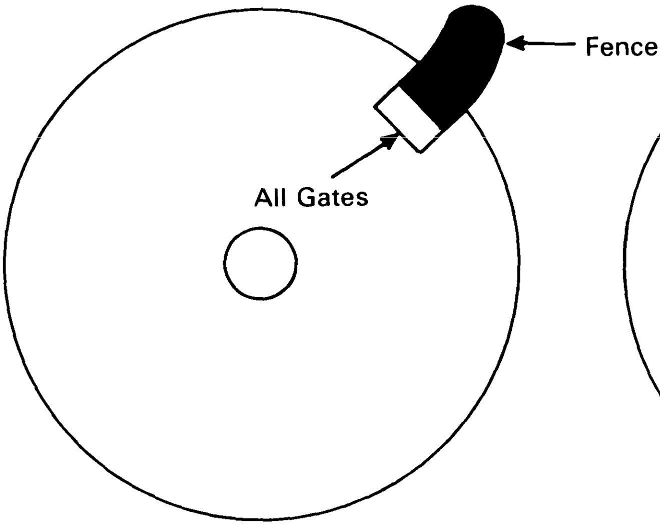


Figure 54—Example of combination lock gates alined and fence in open position.

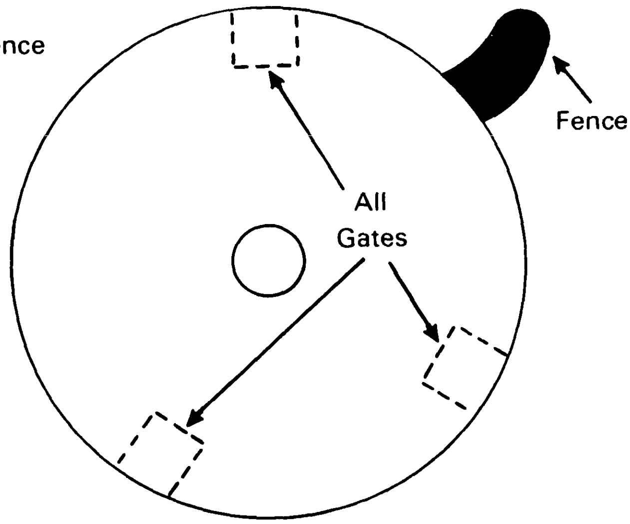


Figure 55—Example of combination lock with gates not alined.

(Figure 54 shows gates and fence in open position.)

(2) Figure 55 portrays improper alinement of gates and fence, caused by applying the wrong combination, preventing operation of the lock.

(3) To determine the number of possible combinations on a lock, you raise the total number of reference points on the dial to the power equal to the number of tumblers. Example: A lock has 40 numbers on the dial and a three-number combination. The three-number combination indicates that there are three tumblers in the lock. Therefore, the number of combinations possible is 40^3 or 64,000. How can someone find one combination out of 64,000 in less than an hour?

(4) On inexpensive combination padlocks there is usually a serial number stamped on the back. These serial numbers can be checked in a code book (available from locksmith supply houses) and the combination of any such lock can be obtained. This is one way an intruder can neutralize the combination lock. Incidentally, a code book for some Master brand combination padlocks can be purchased for very little cost from one major supplier. With inexpensive locks there is a certain amount of tolerance between the widths of the gates and the width of the fence. This tolerance allows for some leeway with respect to the combination numbers. In other words, with these locks, applying the exact combination is not critical. If the exact combination were 1-3-8, for example, the lock might also open on 2-4-7 or 1-4-9. Therefore, manipulation would require the intruder to try every other combination instead of every single one. This cuts the intruder's time considerably.

(5) There are still other ways to neutralize small combination padlocks. The bolt (that part engaging the shackle) is spring-loaded in most models. Therefore, a sharp blow on part of the lock will cause the bolt to jump toward the blow. If this is done properly, the bolt will disengage from the shackle and the lock will open. This operation is known as **rapping.** The combination padlock with the spring-operated bolt can also be opened by

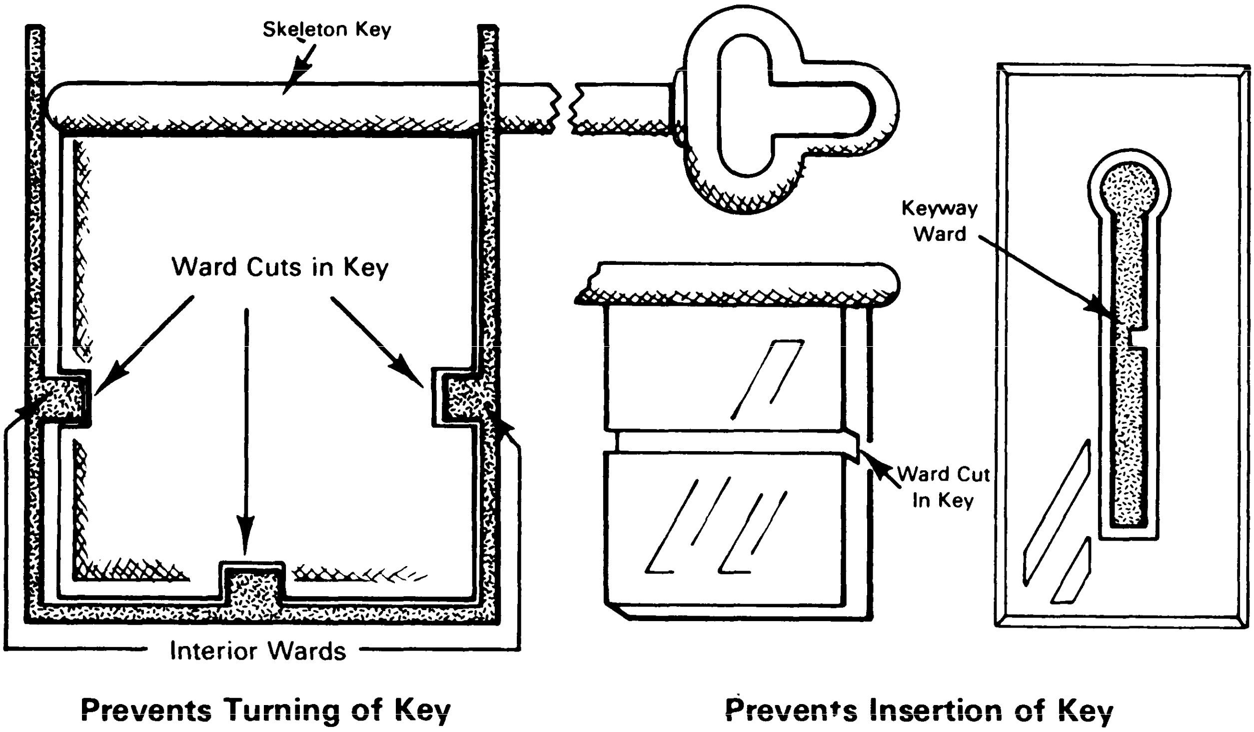


Figure 56—Examples of interior wards and matching ward cuts in keys.

shimming with a small piece of thin metal known as a sneaker. This is an amazingly quiet, simple, and fast operation.

(6) Manipulation can be done on safe locks as well as on simple locks. However, it is not as easy as it appears on TV and in the movies. Most big combination locks employ very close tolerances between gates and fences, balanced tumblers, and false gates to foil surreptitious burglary attempts.

b. Warded locks— While combination locks are popular, key-operated locks are even more popular. One type of key-operated lock is called the warded lock. Wards are defined as obstructions in the keyway (keyhole) and/or inside the lock to prevent all but the properly-cut key from entering or working the lock (figure 56). The key must have the proper ward cuts to bypass the wards in the keyway or in the lock. There are keys made to bypass most wards in any warded lock. These are known as skeleton-keys. However, a skeleton key is not absolutely necessary to bypass a warded lock. A piece of wire bent to the right shape will bypass the wards yet still make contact with the bolt of the lock.

(1) Warded padlocks are frequently seen in barracks and on storage sheds. These locks actually offer very little security. Most are of laminated type construction and to the unaware seem quite secure. They can be identified by a free-turning keyway. An object, such as a nail file, inserted into the free-turning keyway will turn the keyway but will not operate the lock because the keyway is simply a guide for the key, not a functional part of the lock. However, if this object is inserted too far into the lock, it will not turn at all.

(2) Figure 57 depicts a warded padlock. On this type of lock, the shackle is secured not by a bolt, but by a flat spring, the leaves of

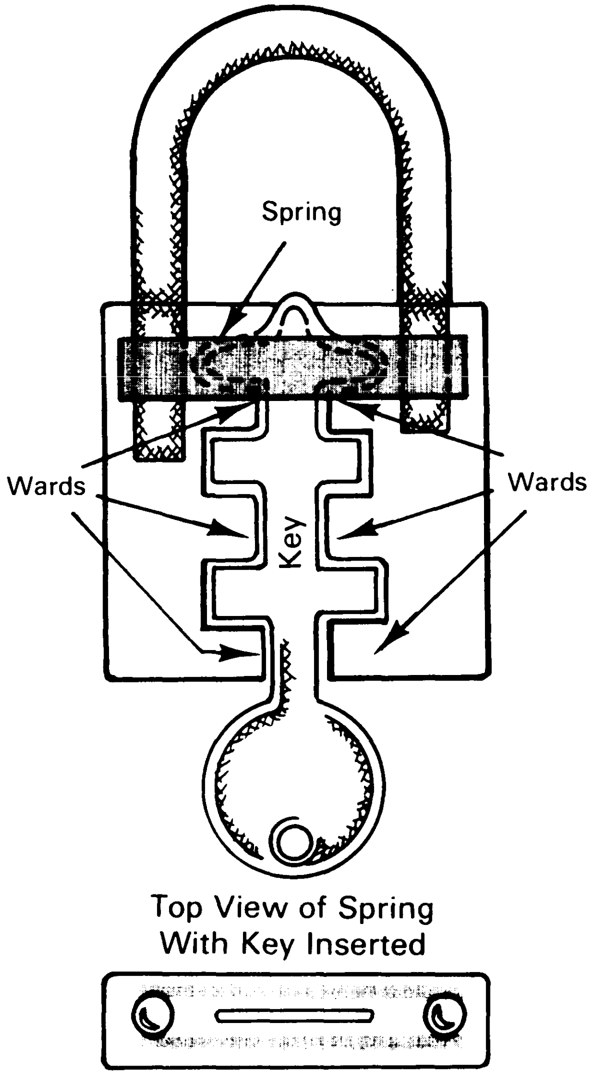


Figure 57— Warded padlocks with spring secured shackle.

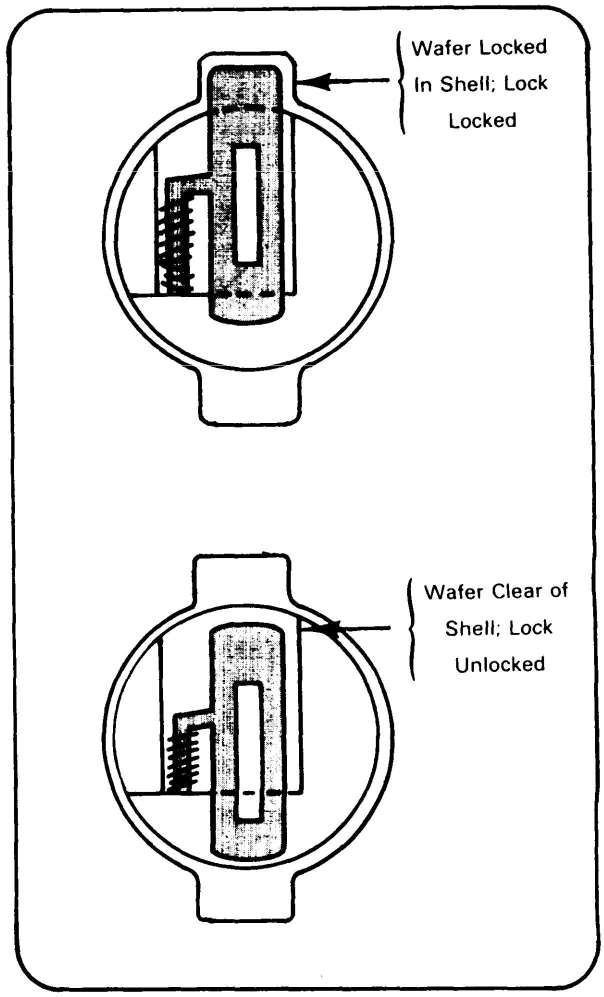


Figure 58— Wafer lock operations.

which press together on the sides of the shackle, engaging a notch on each side of the shackle. To open this lock, all that is needed is to spread the leaves of the spring. This can be done with the proper key, by a specially designed key, or by an ingeniously bent paper clip.

(3) Any lock that relies entirely upon wards for its delay factor is not a good lock for security purposes. Most modern locks employ wards to curtail insertion of unauthorized keys; however, these locks have other security features besides the wards.

c. Wafer or disc tumbler locks— This is another type of key-operated lock. Generally, these devices are more secure than warded locks. Wafer locks are used on most automobiles, desks, cabinets, and in some padlocks. The operation principle of the wafer or disc tumbler lock is as follows: several wafers are located in the core or plug of the lock (the part that turns). The wafers are under spring

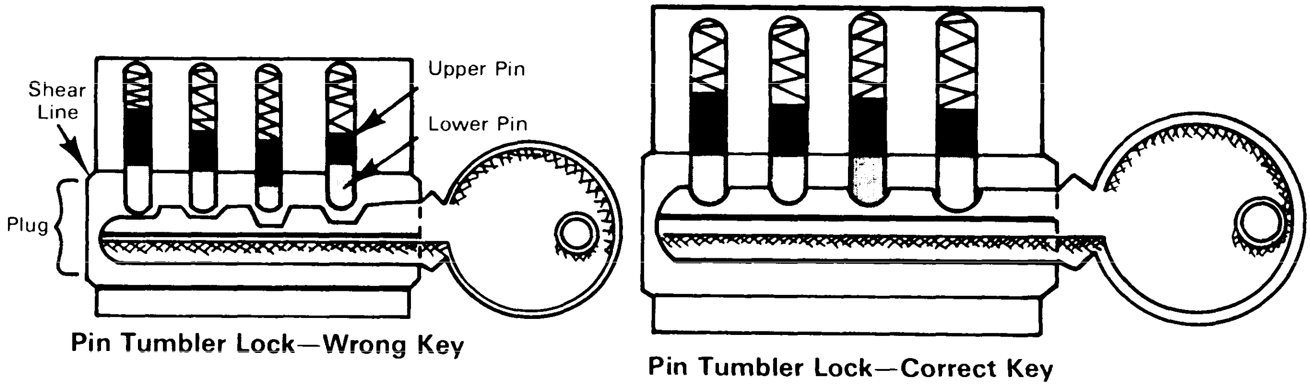


Figure 59—Example of pin tumbler lock operation.

tension and protrude outside the diameter of the plug into a shell formed by the body of the lock (see figure 58, locked), thus keeping the plug from turning and keeping the lock locked. Insertion of the proper key causes the wafers to be pulled out of the shell into the diameter of the plug, allowing the plug to be turned (figure 58, unlocked). If the wafer lock is in a door or a desk and has a spring-operated bolt, it can be shimmed open. If it's in a padlock and has a spring-operated bolt, it can also be rapped open. If it is in a vehicle or if it employs a deadbolt (a bolt which operates only when the key plug is turned) the lock can be picked open.

d. Pin tumbler locks— These are used extensively in commercial, military, and residential security. The pin tumbler lock, generally, is more secure than the warded or wafer tumbler lock. In this lock, pins are moved by a key so that a shear line can be obtained thus allowing the key to turn the plug and operate the lock (see figure 59).

(1) Pin tumbler locks may be incorporated into padlocks, door locks, switches, machinery, etc. The padlocks, if the bolts are spring-operated, may be rapped or shimmed open. In other devices such as door locks, if the pin tumbler lock operates a spring-operated bolt, the bolt may be shimmed open. Specifically, shimming a door open is known as loiding, after the word "celluloid," a material commonly used in this technique.

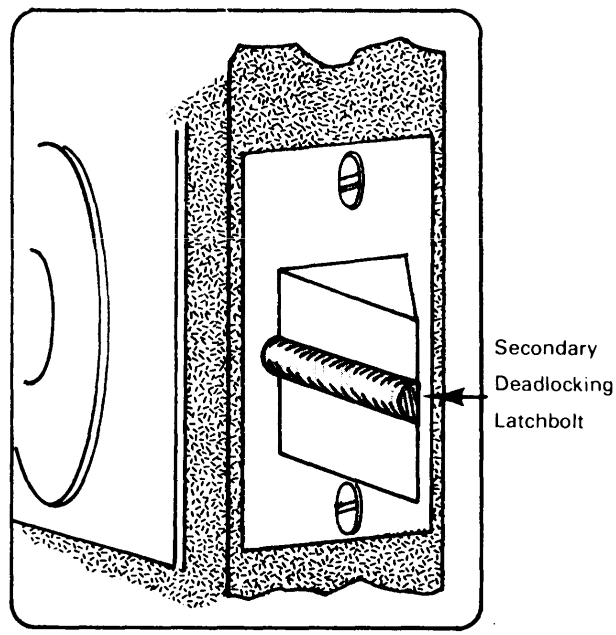


Figure 60—Secondary deadlocking latchbolt.

(2) As in wafer locks, a dead bolt maybe incorporated into a pin tumbler lock to prevent rapping or shimming. The plug of the lock must turn to operate the dead bolt. In this case the lock must be picked. In residential type locks a feature known as a secondary deadlocking latchbolt is often used (figure 60). If properly adjusted so that when the door is closed the bolt is fully extended into the strike (recess for the bolt in the doorframe) and the secondary bolt is

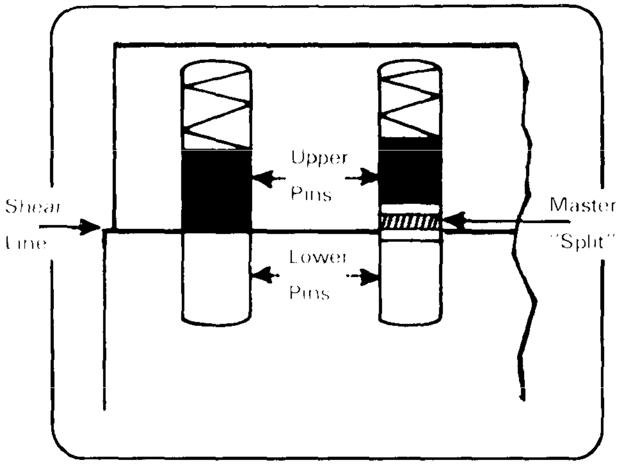


Figure 61—Example of master split in pin tumbler lock.

fully depressed, the secondary deadlocking latchbolt will prevent loiding or shimming. This type of lock should be used on residences—it is cheap security.

(3) The principal operation of pin tumbler locks makes possible the technique of mastering. Mastering allows the use of several differently cut keys to operate the same lock. In mastering (with the exception of one or two particular makes of pin tumbler locks), the pins are segmented by splits which allow several possible pin alinements at the lock's shear line (see figure 61). Because of this, mastering makes picking easier.

(4) To counter this susceptibility to picking, a mushroom or spool tumbler or pin should be used in the lock. This type of pin makes picking considerably more difficult because picking tools tend to cant the tumbler sideways and bind it at the shear line (figure 62). figure 62). The mushroom type pin can also be used effectively in nonmastered locks.

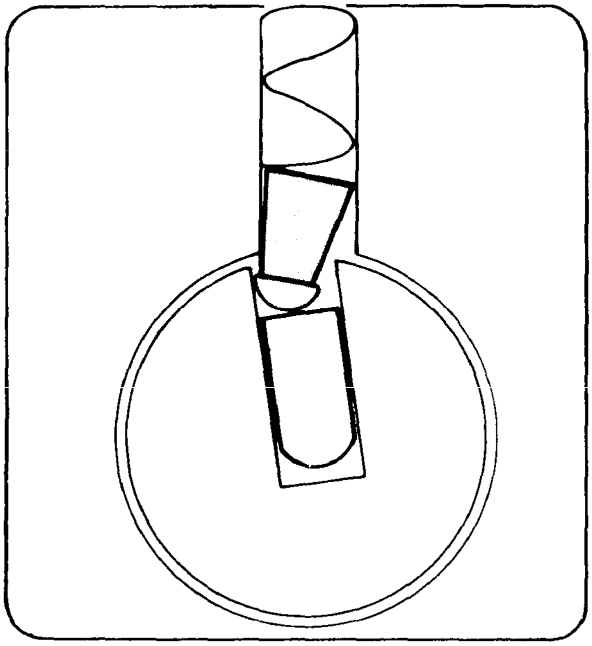


Figure 62—Example of mushroom tumbler action during picking.

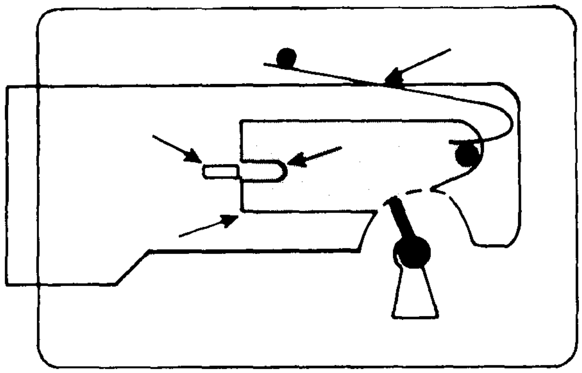


Figure 63—Example of lever lock mechanism.

e. Lever locks— Some locks use a system of levers under spring tension to provide security. The properly cut key will move the levers so the gates will be properly alined with the fence, thus allowing movement of the bolt (see figure 63). Levers are used on some doors (prison type doors) and padlocks. Large lever locks can be made quite pick-resistant since the springs can be made to exert considerable pressure to resist picks. However, lever locks can be picked. If the lever lock has a spring-operated bolt, it can be shimmed or rapped open.

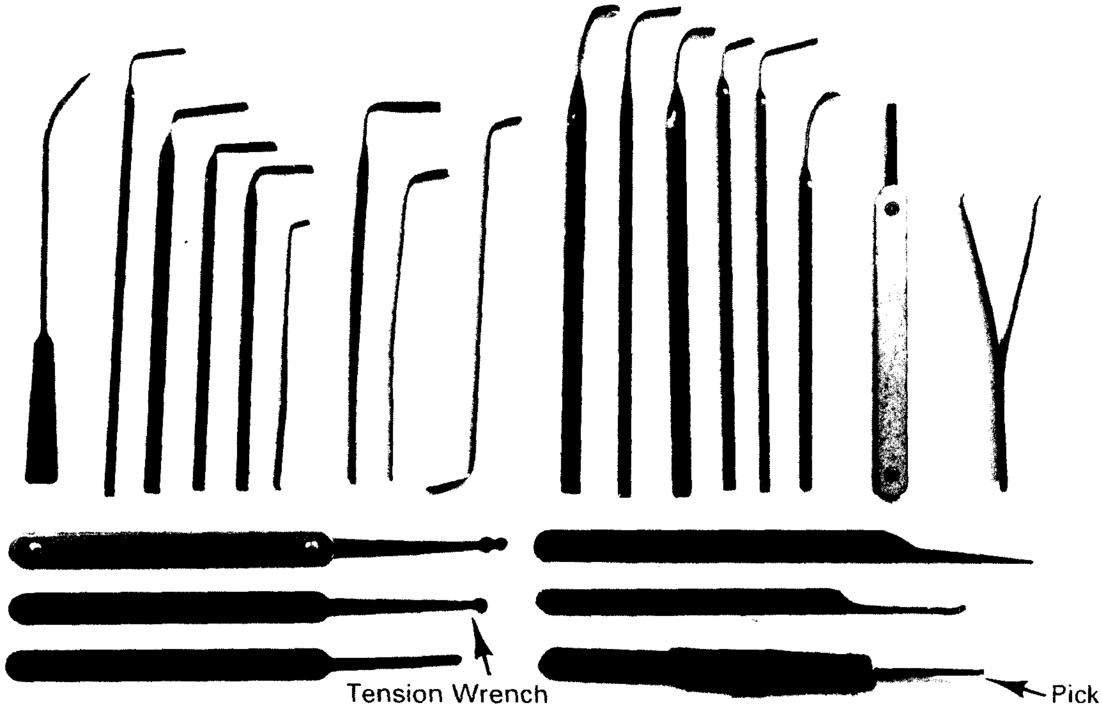


Figure 64—Professional lock picking kit.

8-4 Picking

Since locks are manmade, men can defeat them. For this reason it is foolish to state that a lock is pick-proof. A lock can be called only pick resistant and that is a relative term. In reality, picking is normally quite simple. Picks can be purchased from locksmith supply houses, made at home, or fashioned out, of spoons in confinement facilities.

a. A professional picking kit is shown in figure 64. Basic picking tools are the tension wren ch and the pick. Both are necessary. Without going into detail, the tension wrench imparts a rotary motion to the key plug of the lock and aids in finding the bindings or locking tumblers of the lock. The pick is used to move the binding tumblers, one at a time, to the shear line. When all tumblers are alined properly with the shear line, the lock opens.

b. Picking takes practice, skill, and a little luck. However, it seems that most intruders use other methods to bypass locks. They may cut them, pull them apart, blast them, or rip them off the door. In some doors, the intruder simply spreads the door frame away from the door to release the bolt from the strike. This can be combatted by using locks with long bolts (up to 1 inch) and by using grouting a-round the door frame (this holds the frame rigidly).

c. At times, intruders saw the bolts of locks by putting a saw blade in the space between the door and the frame. Some bolts have floating hardened bearings in the middle of the bolts themselves—this foils the saw attack because the saw cannot get a bite. Hasps are often defeated because they are installed improperly and the screws holding them on the door can be removed.

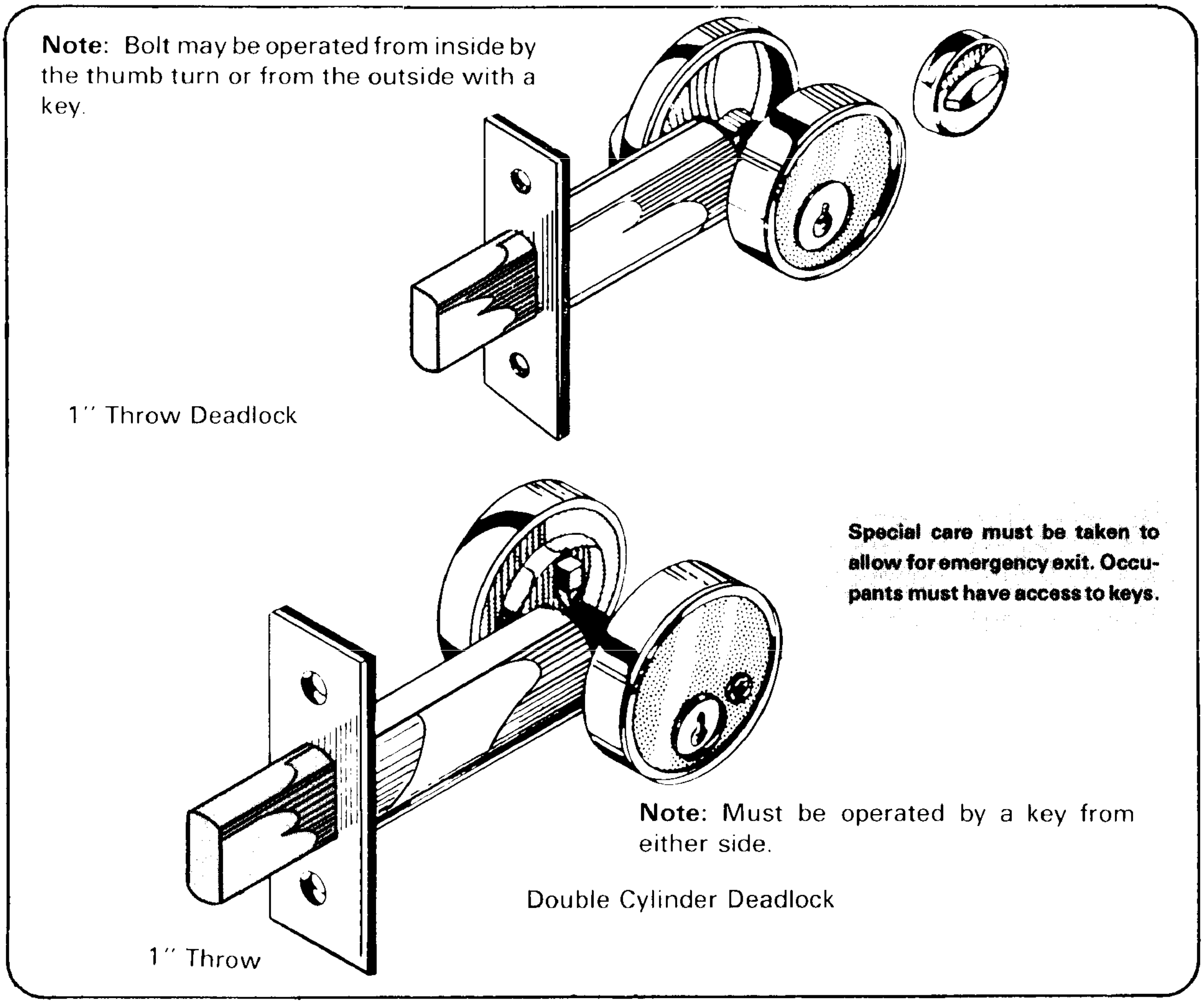


Figure 65—Examples of dead bolt (deadlock) latches.

8-5 Dead Bolt Latches

a. The dead bolt latch may be used on almost any door, is easy to install and inexpensive, and increases the security posture of the facility. For most effective application, the bolt of the latch should be applied so the bolt slides into the door casing frame or into a keeper firmly attached to the frame (not the door facing). Look at the examples of best dead bolt installation in figure 65. The dead bolt latch is recommended for use in military housing as an effective security measure in the installation crime prevention program.

b. Chain latches are not recommended as effective security measures. Because of their usual installation onto door facings, as opposed to door frames, little effort is needed to force entry with a chain latch in the “safe” position (see figure 66).

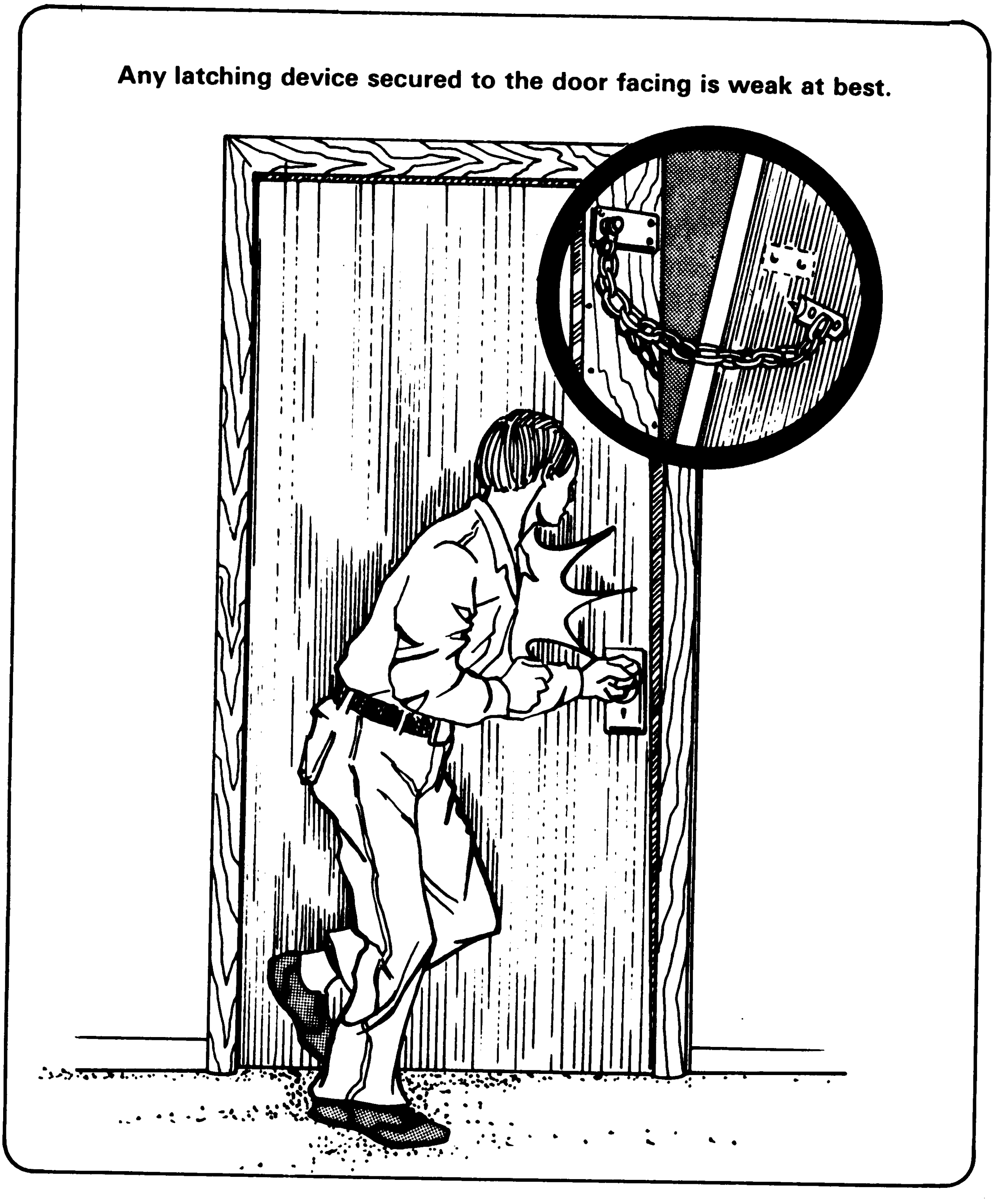


Figure 66—Most chain latches require little effort to neutralize.

8-6 Issue and Control Locks and Keys (General)

Of primary importance in safeguarding property or classified material is a good lock and key issue and control system. Such a system includes control of the combinations of locks.

a. For effective control, accurate records should be maintained and periodic physical inspections and inventories made. The main principles of this system include:

(1) Combinations or keys should be accessible only to those persons whose official duties require access to them.

(2) Combinations to safe locks and padlocks securing containers for classified information will be changed at least once during each 12-month period (AR 380-5), and at such other times as deemed appropriate, and at the earliest practical time following:

(a) Loss or possible compromise of the combination or key.

(b) Discharge, suspension, or reassignment of any person having knowledge of the combination.

(c) Receipt of a container with built-in combination lock.

(3) More frequent rotation of key padlocks may be required in certain instances. This is a recommended practice in all situations.

(4) In selecting combination numbers, multiples and simple ascending or descending arithmetical series should be avoided.

(5) When padlocks with fixed combinations are used with bar locks as supplemental locking devices, an adequate supply should be maintained to permit frequent interchange of locks among users. This type of lock is not considered to provide adequate security unless it is used in large numbers over extensive areas, which permits a successful interchange without compromise. Fixed combination locks should never be used for the protection of classified material.

(6) Records containing combinations should be placed in the same security classification as the highest classification of the material authorized for storage in the container which the lock secures.

(7) Use of keys must be based on the same general concept as applied to safe combinations. Issue of keys must be kept to a minimum and retained under constant key control supervision. Generally, the installation key system should be under control of the installation provost marshal or physical security manager. However, where this is not feasible, the provost marshal should have staff supervision over the system. The following measures are recommended for control of keys to magazines, trailers, warehouses, and other structures containing classified matter or highly pilferable materials:

(a) Keys should be stored in a locked, fireproof container when not in use.

(b) Access lists for persons authorized to draw keys to classified storage facilities should be maintained in the key storage container.

(c) Keys should not be issued for personal retention, or removal from the installation.

(d) Key containers should be checked at the end of each shift and all keys must be accounted for.

b. Key control records should be maintained on all key systems. Accountability can be maintained by records, key cards, and key control registers. Each record must include at least the following information:

(1) Total number of keys and blanks in the system.

(2) Total number of keys by each keyway code.

(3) Number of keys issued.

(4) Number of keys on hand.

(5) Number of blanks on hand for each keyway code.

(6) Persons to whom keys have been issued.

c. Inventories of key systems should be conducted at least annually. Requests for issuance of new, duplicate, or replacement keys should be approved or monitored by the official responsible for key control.

d. A key depository should be provided at installations where keys are secured during nonoperational hours. Supervisors should be required to sign a register for the keys at the beginning of each working day and to turn in keys at the end of the working day. Security personnel should check the key board and register to insure accountability for all keys.

e. Key control systems will normally be engineered to provide the degree of security required with a minimum impairment of the operational mission. Basic requirements for all key control systems are as follows:

(1) High security pin tumbler cylinder locks will normally be specified for use.

(2) Key control systems will be developed to insure against usable keys being left in possession of contractor or other unauthorized personnel. Such assurance is normally achieved by using locks with restricted keyways and issuing new keys on key blank stock that is not readily available to commercial keymakers.

(3) Masterkeying is prohibited except in rare minimum security cases. When pin tumbler systems are masterkeyed, the use of several shorter pins to facilitate two or more acceptable pin positioning reduces the security afforded by use of a maximum number of pins in a nonmasterkeyed lock. One or more mushroom-typed pins or a variation of this type pin will be used in each such lock. Also, individual pins should not be segmented more than two times on those locks being used to secure more sensitive materiel.

(4) All locks (lock cylinders when appropriate) and keys in a masterkeyed system should be numbered with unrelated number system. The words—US government—DO NOT REPRODUCE—should be imprinted on all master and higher level control keys.

8-7 Key Control Officer

a. A key control officer should be appointed by the commander. He maybe the provost marshal, his physical security manager, or other designated individual. This officer should be concerned with the supply of locks and how they are stored; handling of keys; records maintenance; investigation of loss of keys; inventories and inspections; custody of master keys and control keys if applicable; regulations concerning locks and keys on the installation and facility; maintenance and operation of the installation's key depository; and the overall supervision of the key program at the installation.

b. The key control officer should maintain a permanent record of the following:

(1) Locks by number, showing–

(a) Location of each lock;
(b) Key combination, i.e., pin lengths and positions;
(c) Date of last key change.

(2) Keys by number, showing–

(a) Location of each key;
(b) Type and key combination of each key.
(c) Record of all keys not accounted for.

c. The key control officer should also be responsible for the procurement of locks and keys. Based on determined requirements, he should coordinate procurement with the installation or facility engineer, and keep abreast and know the availability of improved locks and keys.

8-8 Mechanics Of Implementation

Since each installation or facility will have conditions and requirements peculiar to its activity, key control systems will vary. Before establishing a system, a survey should be conducted to determine actual requirements and to identify all warehouses, shops, storage areas, safes, filing cabinets, etc., that require the additional protection afforded by locking devices and security of keys. When this determination has been made, an annex to the physical security plan can be prepared to show the following:

a. Location of key depositories.

b. Keys (by building, area, or cabinet number) to be turned in to each depository.

c. Method of marking or tagging keys for ready identification.

d. Method of control for issue and receipt of keys to include maintenance of register and identification of personnel authorized possession of keys.

e. Action required if keys are lost, stolen, or misplaced.

f. Frequency and method of lock rotation.

g. Assignment of responsibilities by job or position title.

h. Emergency type keys, which would be readily available to the security supervisor.

i. Other controls as deemed necessary.

8-9 Keys and Locks For Ammunition Storage (AR 190-11)

a. All doors used for access to arms storage rooms must be locked with approved locking devices. On storage facilities, the locking devices used on the most secure door must be high security padlock and hasp. The secondary padlock, mortise locks, or rim dead locks must be used to secure the other door or the double door requirement. Mortise locks and rim dead locks must meet the following specifications:

(1) Be a key-operated mortised or rim-mounted dead bolt lock.

(2) Have a dead bolt throw of 1 inch.

(3) Be of double cylinder design.

(4) Cylinders are to have five-pin tumblers, two of which are to be of mushroom or spool type drive pin design.

(5) Have 10,000 key changes.

(6) No master keying of lock to be permitted.

(7) If bolt is visible when locked, it should contain hardened saw resistant inserts or be made of steel.

b. At least one lock must secure each door in the triple barrier system. Vehicles and storage facilities in which items are stored must be secured by approved secondary padlocks. Aircraft must be secured with locking devices specified in modification work orders; devices must not be designed and produced locally without approval from the US Army Aviation Systems Command. Doors that cannot be secured from the inside with locking bars or deadbolts will be secured on the inside with secondary padlocks.

c. Keys to arms storage buildings, rooms, racks, and containers must be maintained separately from other keys and must be accessible only to individuals whose official duties require access to them. A current roster of these individuals must be kept within the unit, agency, or organization and must be protected from public view. The number of keys will be held to the minimum. If an alternate set of keys is maintained, they must be secured at the next higher headquarters and inventoried monthly. When the next

higher headquarters is not on the same installation as the unit, the alternate set of keys must be secured by the unit separate from the operational set of keys. Custody of keys will be transferred between authorized individuals after both parties have conducted a visual inventory of weapons, including a total count of weapons on hand. The change of custody and physical inventory must be recorded as prescribed. After duty hours, keys will be secured in a locked container constructed of at least 20-gauge steel or material of an equivalent strength away from the storage area or in the custody of responsible duty officer, NCO, or individuals authorized unaccompanied access. At no time will keys be left unattended or unsecured. Key containers when not in use must be placed in a secure location. Keys to arms storage buildings, rooms, racks, and/or containers must not be removed from the installation. The use of master key system is prohibited. In the event of lost, misplaced, or stolen keys, affected locks or cores to locks must be replaced immediately. Replacement or reserve locks, cores, and keys must be sufficiently secured to preclude them from being readily accessible to unauthorized individuals.

d. A key and lock custodian must be appointed and his or her duties will include insuring the proper custody and handling of keys and locks. A key control register must be maintained at all times to insure administrative accountability for keys. Key control registers must contain the signature of each individual receiving the key, date and hour of issuance, serial number of key, initials of person issuing the key, date and hour key was returned, and signature of the individual receiving the returned key. Key control registers must be retained in unit files for one year and then destroyed.

e. Organizations or agencies maintaining keys to arms storage buildings, arms storage rooms, and arms racks must establish a key control accountability system which will include, in addition to the key control register mentioned in paragraph c above, records that identify:

(1) Total number of locks and keys in the lock system used by the organization or agency, including replacement or reserve locks.

(2) Total number of keys for each lock.

(3) Number of keys issued.

(4) Number of keys on hand.

(5) Number of keys and locks retained in reserve.

(6) Persons to whom keys have been issued.

f. Padlocks must be locked to the staple or hasp when the area or container is open to preclude theft, loss, or substitution of the lock.

g. Inventories of keys and locks must be conducted semiannually. Inventory records must include the information contained in paragraph e, above, and be retained in unit files according to regulations.

h. Combinations to locks on vault doors or class V containers will be changed semiannually and the combinations safeguarded in accordance with AR 380-5. Padlocks used to secure entrances to arms storage facilities must be rotated at least semiannually, and a record maintained reflecting the date of rotation. All other locks used to secure weapons will be rotated at least annually. Rotation of locks will be such that none of the locks formerly used to secure the doors, racks, or containers securing weapons will be used, after rotation for a period of 3 years, within the same arms storage facility. Rotation will include exchange of locks among units or from another geographical area. Each arms room will maintain on hand a back-up set of locks amounting to 15 percent of the number of locks in use. Keys to locks to be used must be inventoried at the time of rotation. The loss of or inability to account for any key to a lock makes that lock unauthorized for the purpose

of securing arms or ammunition. Lock combinations will be changed—

(1) When placed in use after procurement.

(2) At least semiannually.

(3) On transfer, reassignment, resignation, or relief of any person having the combination.

(4) When the combination has been compromised or the lock has been found unlocked and unattended.

8-10 Lock and Key Control For Nuclear Storage (AR 50-5)

a. Each nuclear weapons storage structure entrance in a permanent exclusion area must be locked with at least two key-operated high-security padlocks with shrouded shackles which meet military specification MIL-P-43607 (GL) and with appropriate style high-security hasps, as described in amendment 1 to this military specification.

b. A custodian must be designated by the commander to control, issue, and maintain adequate records of all keys and locks to buildings or areas containing nuclear material. Keys must be made available only to designated personnel whose official duties require access to them. Key registers, to indentify keys for each lock, their current locations, and custody, will be maintained. Repositories must be provided in areas where keys are secured during nonworking hours. Key repositories, racks, boxes, rings, and boards will be secured when not in use. All keys must be jointly inventoried with each change of key custodians. Keys stored in two-man control containers need only be inventoried when containers are opened. Keys and locks must be inventoried every month and must be given routine maintenance at that time. The number of installed padlocks should be supported with a 5 percent backup of serviceable padlocks.

c. Active entrances to all permanent storage structures must be equipped with dual high-security locking systems or one high-security locking system equipped with an anti-tamper device. All other exterior storage structure doors must be secured by a substantial dead-bolt device from inside the structure.

d. No one individual may have access to or possession of the keys to both locks of a structure containing nuclear weapons. Keys to nuclear weapon storage structures must be controlled as classified material at least equal to the classification of the material being protected.

e. Key padlocks must be changed, have their cylinders replaced, or be rotated randomly between structures or sites at least annually. They must be replaced upon loss or compromise of their operable keys. Rotation of padlocks is not required when either of the following exists—

(1) Two padlocks are installed on each structure and a system established for separating these locks into A- and B-series locks. Personnel must be identified and authorized to have in their possession the keys to either the A-series locks or the B-series locks, but not both.

(2) The locking mechanism is protected by an anti-tamper bar that will activate an alarm when it is moved.

f. Master keys are prohibited.

g. Keys to currently installed locks must not be removed from the site.

h. Keys and spare locks must be protected in a secure container when they are not needed for authorized operational purposes.

8-11 Inspection Procedures for Defective Locks

a. A periodic inspection should be instituted upon all locks to determine the locking mechanism's effectiveness, detect tampering, and to make replacements. This may be accomplished by inserting a test key (any comparable key other than the assigned key) no more than one-quarter inch into keyway. Turn test key by hand using the normal amount of force required to open lock. If the lock opens during inspection, it should be replaced immediately. Care must be taken during inspection to prevent jamming of test key into key recess. Jamming will cause severe damage to locking levers and may preclude removal of test key.

b. Defective locks. Locks found defective during test inspections must be reported to Defense Industrial Supply Center (DISC) on SF 368, Quality Deficiency Report. Defective locks will be retained until disposition instructions have been received.

c. Periodic maintenance. In addition to the above, periodic preventive maintenance of locks should be performed to insure adequate lubrication, employment of rust preventive on outer surfaces and clearing of dust and moisture from keyways.

Chapter 9

Security Forces



The security force of an installation or facility provides the enforcement medium in the physical security program. This force consists of persons specifically organized, trained, and equipped to protect the physical security interests of the command. It is a commander's most effective and useful tool in a comprehensive integrated physical security program.

9-1 Types of Security Forces

a. Military.

(1) On an installation or facility, military security forces may be military police or they may be from other branches.

(2) The interior guard type of security duties are performed by installation or facility unit troops on a roster basis. Military police normally perform security duties that require higher degrees of training and experience, such as:

- Security of restricted areas.
- Security of specific sensitive gate(s).
- Supervisory or coordinated role with other military or DOD Civil Service Security Guards.

(3) Depending on the mission, area, facilities and/or functions to be secured; enemy situation; and similar factors, a military police unit may perform the entire physical security function. When it cannot assume responsibilities for all of the physical security requirements in the command, other physical security forces must be required.

(a) These additional forces may consist of personnel furnished by other units of the command on a daily, weekly, or other periodic basis. While this method has the single advantage of providing additional manpower, it has the disadvantages of rapid turnover and lack of training of such personnel in security requirements and procedures. If used, such personnel should be assigned the least sensitive posts or patrols.

(b) The military police unit may be augmented either by over-staffing if qualified personnel are available, or by activation of a provisional unit(s) under the provisions of AR 220-5. Such a unit may be of any size (such as platoon or company).

- This type of action must be approved by the senior commander from whose resources the personnel will be drawn.
- This method has the advantage of providing a more stable force than described in paragraph 9-1a(3)(a) above and an organizational framework in which training and operations can be more realistically blended.
- The disadvantages of this type unit are that it is considered only a temporary measure, and the personnel are obtained only on a temporary duty or detail basis from their parent units. It is intended for use only in unforeseen circumstances and for temporary periods. Should a continuing need be anticipated, action should be initiated for activation or assignment of additional military police TOE/TD units or other security guard type units.

(4) Another source of physical security forces is the combat arms branches, especially the infantry. Units of such branches may be attached to military police units, and as such, may be designated as security guards and assist in all required and appropriate operations.

(5) A final source of military forces maybe the host country in an oversea area.

Military or paramilitary units of the host country may also be attached to, or operate in coordination with, military police. They may also be supplemented with national police of their own country.

b. Civil Service. These security personnel are uniformed civilian employees of an agency of the government. They are customarily trained and organized along semimilitary lines. The organization may be completely civil service or may be composed of civil service personnel under military supervision. In either case, it is under operational control of the provost marshal or security officer.

c. Labor Service Personnel. In addition to military and civil service forces, labor service type units composed of local civilian personnel have been organized and used successfully in a theater of operations. These types of units were organized after World War II and since that time have established enviable records in the physical security field. These personnel, men of many nationalities, are distinctively uniformed, organized, and equipped. They have set and maintained the highest security standards, resulting in a very minimum loss of property. While not military organizations as such, these units have successfully developed a high sense of duty and esprit de corps, which has been reflected in their outstanding contributions to the physical security of installations in oversea commands.

d. Auxiliary Force. It maybe advisable to have an auxiliary force to supplement the regular force and to relieve the regular force for additional duties which may be required during a disaster or national emergency. Auxiliary force personnel should be drawn from installation or facility personnel.

(1) Retired military personnel may be used if they are physically capable.

(2) The auxiliary force should be organized in the same manner as the regular security force.

(3) It maybe necessary to train certain of the regular force in supervisory positions so a nucleus of supervisory personnel is available to staff the auxiliary force in case the need for their service arises.

(4) Auxiliary forces should be adequately trained and equipped to be able to function effectively. A uniform, or at least a distinctive arm band, should be provided. Arms and other necessary equipment can be issued as needed from regular supply channels. An intensive training program should be set up whereby each auxiliary receives at least the basic training of a member of the security force and periodic refresher training.

(5) If auxiliaries are employees, this training should be accomplished during normal working hours so as to interfere with their normal working schedule as little as possible.

(6) Such use of nonmilitary personnel must be closely coordinated with the personnel officer and the G1, as to employment aspects; and with the staff judge advocate as to legal aspects (such as liabilities, responsibilities, etc.).

9-2 Authority and Jurisdiction

It is most important that the provost marshal or security officer determine (and instruct his security force in) the extent and limitations of the commander's jurisdiction in the field of law enforcement and investigations.

a. Jurisdiction of Place.

(1) Military installations and facilities. Whether state or Federal law or both are applicable on a particular portion of a military installation or facility depends largely on the nature of jurisdiction over the land involved. The amount of Federal jurisdiction will vary between different areas of the same installation or facility.

The legal formalities of acquiring jurisdiction over land under the control of the Secretary of the Army are accomplished at Department of the Army level and in accordance with the provisions of AR 405-20. Information and advice relating to jurisdictional questions should be obtained through the office of the local staff judge advocate. If the required information is not available in that office, it will be furnished to the staff judge advocate by Lands Division, Office of the Judge Advocate General.

(2) Areas outside military installations. Areas outside military installations are generally subject to state and local law. However, there are exceptions. Information and advice in this regard should be obtained through the local staff judge advocate.

(3) Oversea areas. In oversea areas, jurisdiction of place varies according to the military situation, and existing international treaties, contracts, and agreements. Guidance should be obtained in each instance and area from the commander and the staff judge advocate, and set forth in appropriate command directives.

b. Jurisdiction of Persons.

(1) Jurisdiction of persons follows, in general, the limitations of jurisdiction of place.

(2) Military police have jurisdiction and authority over persons as described in FM 19-5 and related publications.

(3) The source of authority for Federal civilian employees assigned to security, police and guard duties is derived from the commanding officer of the installation. These personnel can have no more authority than he possesses and are subject to any limitations imposed thereon.

(a) Security force personnel may enforce all offenses under the UCMJ, military regulations, Federal law and regulations, and state law where applicable.

(b) Security force personnel may be given the same authority as MPs over all personnel subject to military jurisdiction, including apprehension, detention, search, and interrogation.

(c) Security force personnel have no specific grant of authority over civilians other than the right of citizen's arrest, which every citizen enjoys.

- They maybe deputized in accordance with state authority where applicable, but only upon prior permission from DA and must serve in that capacity without extra compensation. (See Federal Personnel Manual § 734.101.)
- Department of Justice policy is against deputizing such personnel as US Marshals. (See Op JAGN 1952/82, 2 Dig Ops Posts, § 23.1.)

(4) The commander is the source of jurisdiction and authority for all other personnel assigned to security force duties.

9-3 Personnel Selection

Regardless of the use of structural, mechanical, electronic, and other supplements, the human element in security operations makes the difference between success and failure. Commanders and supervisors have a definite responsibility, under the provisions of AR 604-5, to insure that security personnel who control access to restricted areas and classified activities are screened, selected, cleared, retained, or disqualified, based on criteria contained in that regulation.

a. Desirable Qualities of Security Force Personnel. Most of the qualities desired in security personnel are developed through training and become instinctive through experience. Every person assigned to security duties must recognize the part he plays in this development; he must have an

Security Force Qualities

Alertness	Tactfulness	Trustworthiness
Sound Judgment	Self-Control	Reliability
Confidence	Loyalty To Job	Security Clearance
Physical Fitness	Responsibility	Good Mental Attitude

awareness of his need to acquire this instinctiveness and a willingness to learn principles of self-improvement. Many qualities are desirable for security personnel; however, only those considered essential for key performance of security duty are outlined below:

(1) Alertness. This quality, more than any other, will determine the effectiveness of a person assigned to security force duties. It must be cultivated by all security force personnel. Even though hundreds of contacts are made with individuals who show proof of the right and need to enter a restricted area, for example, one contact could be with a person who should not enter. To be able to detect this one exception, the security guard must be constantly alert.

(a) He must watch for deviations from the normal, such as a strange car near his post, a person approaching from an area which is not normally used, or nervousness in an approaching individual.

(b) Little things that seem to have no significance may add up to something important. Alertness can be achieved only by keen watchfulness and by diligent application to the requirements of the patrol or post.

(c) Technological advancements in communications equipment and protective alarm systems enhance the effectiveness of security forces; but nothing can be substituted for the alertness of security force personnel. Alertness makes the difference between effective security and a lack of security.

(2) Judgment. Sound judgment is more than the application of common sense—it is the power of arriving at a wise decision. The process involves mental comparison of an unfamiliar situation with a similar situation of known values and relationships. With careful discrimination during the process of elimination, the formulated decision will be sound. It follows that knowledge precedes judgment, and experience provides knowledge. Both are necessary. Security instructions cannot cover each situation. They can provide only fundamental guidelines, because each situation is unique and requires individual consideration. Each guard must develop the ability to observe, compare, and discriminate similarities and differences. However, a word of caution is in order: **security personnel should be trained to call security headquarters for instructions when in doubt as to a situation or experience.**

(3) Confidence. This quality is not

inborn-it is learned. Confidence is a state of feeling sure, a state of mind free from doubt or misgivings. Confidence includes faith in oneself and in one's abilities, and nothing can bring out self-confidence like job knowledge. Each man must have confidence in himself, his weapons, his leaders and other members of the security team. Confidence is thus best achieved through thorough and proper training and competent supervision.

(4) Physical fitness. Security duty is difficult and demanding. The security of an installation or facility-and even the life of the person assigned to security duties-may depend upon his physical fitness. Training in the techniques of unarmed defense and in physical conditioning is essential for developing this quality.

(5) Tactfulness. The ability to deal with others without giving offense is a quality desired in security personnel. It is difficult to assume the authority and responsibilities of security duty without consciously or subconsciously displaying a sense of superiority and an overbearing manner. Security personnel must be able to give instructions clearly and concisely, firmly, and authoritatively, but without arrogance.

(6) Self-control. Security duty presents situations which require not only sound judgment and tact, but also self-control. When an individual is offensive, the security guard must be impersonal in his response, or he will likely lose control of his temper and of the situation. The security guard, after he has given his instructions, should keep his conversation to a minimum. A person who is trying to beat the system will attempt to make the security guard angry. A person on the defensive does not have the situation under control. This situation will occur most frequently in making apprehensions, issuing traffic citations, and during civil disturbances.

b. Other Requirements.

(1) In selecting personnel for security force assignment and in their continuing performance, each man's general mental attitude toward life and his job is most important. Uncompromising interest and loyalty to the job are particularly applicable to security personnel. Supervisors must be alert for any change in this attitude that might adversely affect the performance of security personnel.

(2) Only personnel of known responsibility and trustworthiness should be assigned to security duties. Security clearance criteria for security positions must be based principally on the security classifications of the information to which access will be granted. Security positions are normally designated as sensitive, and require a security clearance of SECRET. Army Regulations 381-130 and 604-5 describe criteria and procedures governing security clearances for military personnel and affiliated civilians. Appropriate civilian personnel regulations should also be consulted where civilians are involved.

(3) Requests for security clearance must be processed in accordance with the above cited regulations.

(4) Positive evaluation of the reliability of all personnel must be made before they are entrusted with access to classified or sensitive information and followup action must be made on all personnel who are granted security clearance to insure that their actions are above reproach. Those personnel not meeting or adhering to the prescribed standards must have their security clearances revoked, and thereby lose their access to areas containing classified information or material (AR 604-5).

c. Women. Security positions maybe efficiently filled by women. Women are required where search of females is necessary.

9-4 Organization and Employment of Forces

The discussion in this section is directed primarily toward physical security in a static situation, such as a CONUS installation or facility. Some of the factors discussed are applicable in other situations, such as in an active theater of operations; others are not.

a. Organization. The organization of a security force will vary depending on circumstances and forces available. Forces may be organized by:

(1) Fixed post deployment.

(2) Patrol deployment.

(3) Reserves.

(4) Any combination of these three.

b. Manpower Requirements. These requirements for a security force will vary according to the types of operations being performed. A method for computing requirements is shown in the following example (see also ARs 310-31, 570-2, and 570-4):

(1) Function: physical security.

(2) Work activity: fixed security post.

(3) Work unit: fixed security post. Post is operated on a continuing basis, 24 hours a day, 365 days a year, with 2 men on duty at the post at all times.

(4) Performance standard: 52.8 man-hours per fixed post per day.

(5) Productive hours per man per year: 2,753 man-hours. Based on 12-hour shifts, 4,380 man-hours are available per man per year. Of this total, 1,627 man-hours are nonproductive by reason of preparation for duty, maintenance of equipment, briefing, travel to and from posts, and similar requirements.

(6) Formula for determining authorization criteria (also see chapter 2):

$$\frac{\text{Man-hours required per post per day}}{\text{Productive man-hours per man per year}} \times \text{Operational days per post per year} = \text{Number of direct workers required to man one post}$$

(7) **Computation:**

$$\frac{52.8 \times 365}{2{,}753} = 7 \text{ direct workers per post}$$

(8) **Authorization criteria:** Seven direct workers for each two-man post.

c. Shifts. Security forces are normally organized into three or four shifts, usually on duty for eight-hour periods. Normally, one individual is placed in charge of each shift of the force. Clear and definite understanding should exist as to seniority and who is in charge of the shift. Changes of shifts should occur before peak periods of activity in the normal operation of the installation or facility. The minimum requirement of security personnel for each shift should be established by dividing the total number of man-hours needed by hours in the shift. To this number must be added sufficient manpower to provide relief, which is usually based on one-half hour per man needed for each shift. If there is a post or patrol requiring less than 8 hours duty occurring during a shift, this security may be provided by drawing a man or men from a less essential mission, or by adding personnel to the shift and using their services in some other post on patrol, or as relief during extra time.

9-5 Security Force

a. Instructions to the security force should be issued in writing. These instructions are normally in the form of General, Special, or Temporary Orders, and should be carefully and clearly worded to include all necessary phases of each assignment. They should be reviewed at least monthly to be certain they are current. Categories of instructions and the scope of each are as follows:

(1) General Orders are those which concern the security force as a whole and are applicable at all posts and patrols. They must cover such items as wearing of the uniform, reporting for duty, report writing, etc.

(2) Special Orders pertain to the conduct of a permanent post or patrol. Each permanent post or patrol should have Special Orders issued concerning the location, duties, hours manned, arms, ammunition and other equipment required, and instructions on the use of force in enforcement and apprehension activities.

(3) Temporary Orders are issued for a short period covering a special or temporary situation and having no permanency at the time issued. If it can be predetermined, such orders should indicate the period of time for which they are valid.

b. A security force manual or handbook covering standing operating procedures, and setting forth policies, organization, authority, functions, and other required operating information, should be prepared and distributed to each member of the security force for required reading. Each man should be held responsible for full knowledge and understanding of its contents. Each installation provost marshal, physical security officer, or chief of guard force, should conduct periodic inspections and examinations to determine each individual's degree of understanding of and compliance with all security force instructions.

9-6 Headquarters And Shelters

a. Location of the security force headquarters will depend on the size and layout of the installation or activity. The objective is efficient control of the security force, and adequate security of vital activities. On a small installation there is frequently only one full-time entrance, which may be supplemented by several part-time

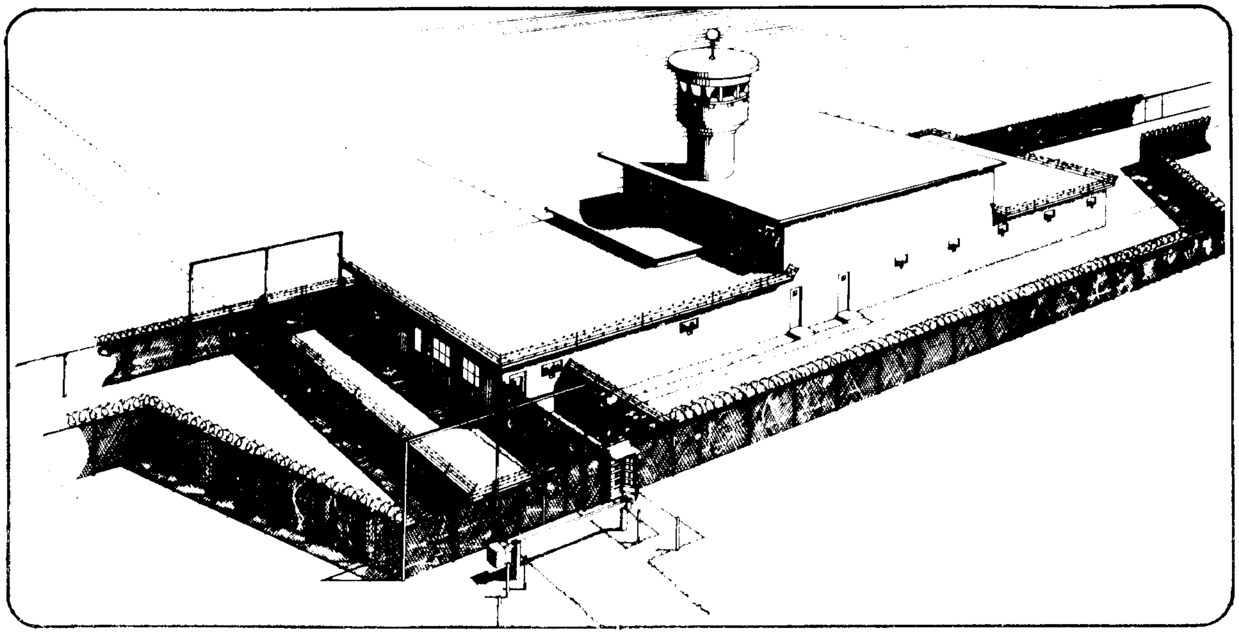


Figure 67—Location of security forces and headquarters.

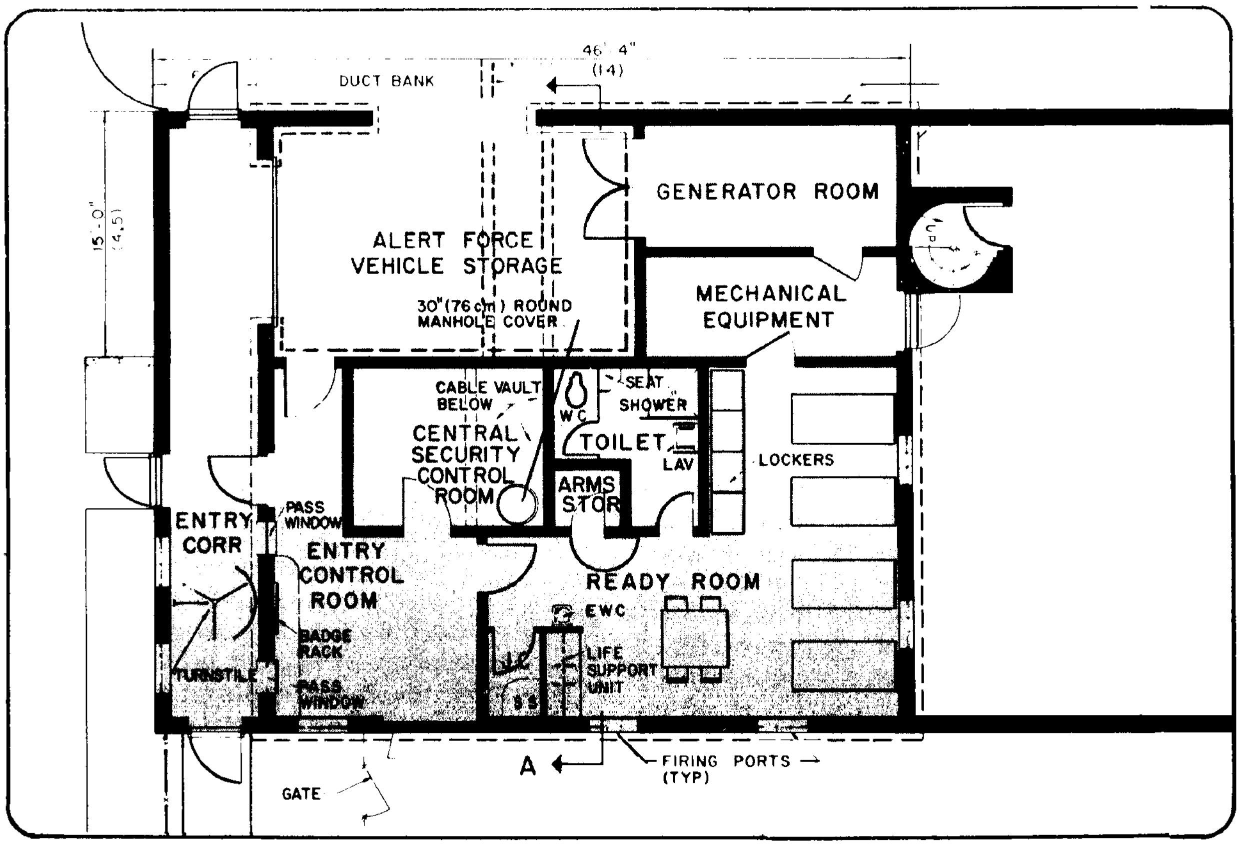


Figure 68—Floor plan for security force headquarters.

entrances. At such an installation the logical location of the headquarters would be at or near the main entrance. On the other hand, at an installation of large acreage it might be much better located near the center of the main group of buildings.

b. The security force headquarters should be the control point for all matters pertaining to physical security of the installation and the terminal or monitoring point for protective alarm and communication system (see figures 67 and 68, page 162).

c. A list of key telephone numbers should also be available for use in emergency operations. It is frequently the office of record on security matters, and usually houses the pass and badge office with its identification and visitor control files. It should have a reliable and independent means of contact with nearby civil authorities.

d. Personnel shelters should be designed to provide occasional temporary protection from severe weather. The design should include space for one person only; facilities such as heat, ventilation, storage space for essential accessories, and lighting that will not expose the occupant; and good visibility in all directions (see figure 68). (For towers, fence, and protective lighting, see chapters 5 and 6.)

9-7 Execution Of Security Activities

a. Security personnel should definitely and clearly understand their **relationship to employees.** They have certain duties to carry out in respect to employees, but bad employee relationships can result if security personnel become impertinent and assume powers not rightfully theirs.

b. Security personnel must understand the methods and techniques that will detect security hazards and assist in identifying violators and intruders.

c. Written reports should be required for all security activities. These should be prepared by each man and turned in to the supervisor for necessary action.

d. Personnel who are assigned to fixed posts should have some **designated method of securing relief** when necessary. Where fixed posts do not permit the person to move at all, such as posts on watch towers, arrangements should be made so they may leave their posts at least every two hours.

e. A simple but effective **plan of operation** should be worked out for the security force to meet every foreseeable emergency. Practice alarms should be conducted frequently to test the effectiveness of this plan and the understanding of it by the security force. Such plans should be designed to prevent a diversion at one point in the installation, drawing off the guards and distracting their attention from another section of the installation where unauthorized entry may be made.

f. Routes for security patrols should be varied at frequent intervals to preclude establishing a routine which maybe observed by potential intruders and used to gain entrance.

g. Records of tours and reports to headquarters should be carefully checked. Failure to record a visit at a designated station, to report to headquarters as required, or any other deviation from established reporting procedures should be investigated immediately. (1) Security personnel should have no firefighting or other similar duties regularly assigned. Such emergencies offer an excellent diversion to cover the entrance of a saboteur or pilferer. Consequently, during such times security personnel should be exceptionally alert in the performance of their duties. (2) It must be strongly emphasized that security personnel will be used for

security duties and should not be given other routine functions except as directed by the commander or his representative. (3) They may and should, however, be given cross-training in other areas such as firefighting, so they maybe used when required and when circumstances permit (such as when off duty).

Training

Section III

9-8 Training Requirements

The extent and type of training required for security forces will vary according to the importance, vulnerability, size, and other factors affecting a particular installation or facility. The objective of the training program is to insure that all personnel are able to perform routine duties competently and to meet emergencies quickly and efficiently.

9-9 Benefits Of Proper Training

a. Efficient and continuing training is the most effective means of obtaining and maintaining maximum proficiency of security force personnel. Regardless of how carefully a supervisor selects personnel for his force, seldom do they initially have all the qualifications and experience necessary to do the job well. In addition, new and revised job requirements frequently mean that personnel must be retrained for different jobs and skills. The gulf between ability and job requirement can be bridged by training.

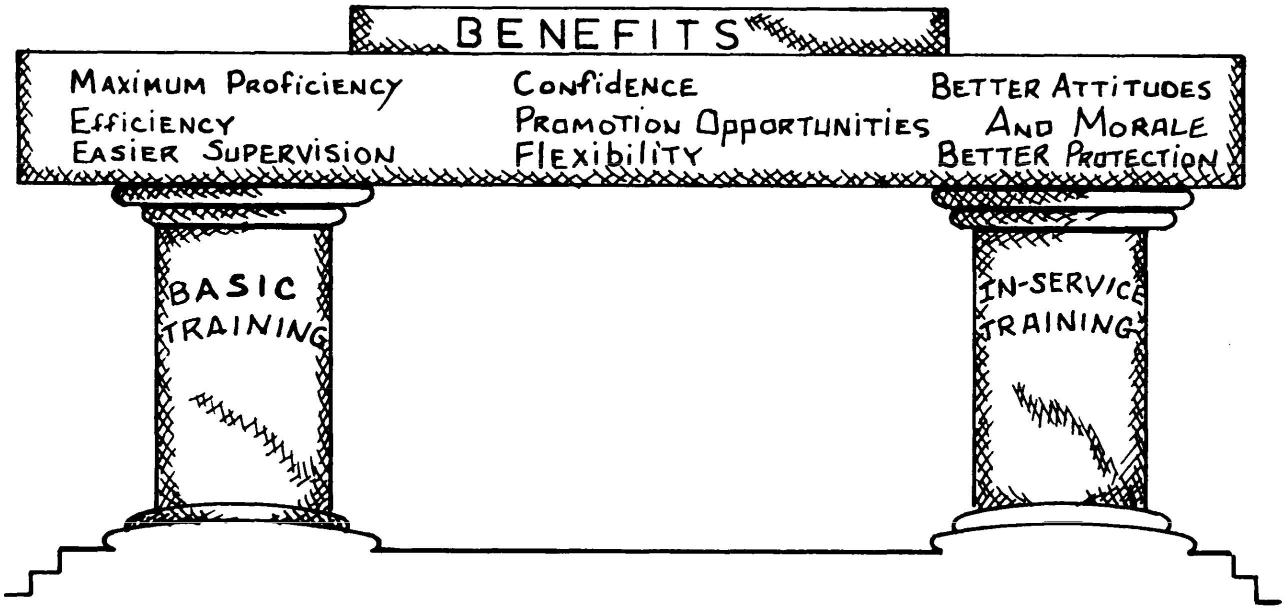
b. It is also well for supervisors to remember that all people do not have the same training needs. It is a waste of valuable time to train an individual in subject matter which he has already mastered, and it is a source of dissatisfaction to the man when he is subjected to instruction that he knows is not appropriate to his skill level. Past experience, training, acquired skills, and duty assignments should be evaluated for each person as an aid in planning an effective training program.

c. A good training program has benefits for both the installation and the security force. Some of the benefits are:

(1) For supervisors. The task of supervising the security force is made easier. There is much less wasted time. Fewer mistakes are made. The resulting economies of motion or action are of benefit to the installation. There is also less fiction with other agencies. A good program also helps to instill confidence, which is most valuable to a security force.

(2) For security personnel. Training benefits personnel because their skills are increased; it provides increased opportunities for promotion; and it provides for better understanding of their relationships to the command or management.

(3) For the security organization. Good training helps to provide for more flexibility and better physical protection, fewer required personnel, and less time required to learn duties and requirements. Training also helps to establish systematic and uniform work habits. An effective program helps to create better attitudes and morale.



9-10 Basic Training

a. Military police personnel assigned to physical security assignments, as a minimum, have completed basic training and advanced individual training. Dependent on their experience, they may need special training in physical security or only such additional training as required by the peculiarities of the installation.

b. As a minimum, personnel (including civil service security personnel) who have not had security police training should receive training at their assigned units or agencies in their security duties, to include:

(1) Care and use of weapons. No man should be placed on security duty unless he has completed at least familiarization firing within the past 12 months with the weapon with which he is armed. Weapons training must also include thorough indoctrination and understanding of the provisions of AR 190-28, concerning the use of force by law enforcement and security personnel.

(2) Area of **responsibility and authority** of security personnel, particularly on apprehension, search and seizure, and the use of force.

(3) Location and use of **first aid and fire control** equipment and electrical switches.

(4) Duties in event of **emergencies,** such as alerts, fire, explosion, civil disturbance, etc.

(5) Common forms of **sabotage and espionage** activity.

(6) Location of **hazardous and vulnerable equipment** and materiel.

c. Army Training and Evaluation Program (ARTEP 19-97).

d. Special training to fit individual situations may be required at installations where security duties are unusually varied or complex. Key personnel should be chosen to attend specialized security courses available at the US Army Military Police School/ Training Center, Fort McClellan, Alabama; or specialized oversea command courses. Extension courses covering physical security subject matter are also available for all personnel on a self-study basis from

ACCP, US Army Training Support Center, Newport News, VA 23628.

9-11 In-service Training

a. When a new individual is assigned, he must be given instruction in conditions peculiar to his post. Whenever possible, his first assignment should be with an experienced man. Additional in-service training and periodic retraining to review basic material and such other subjects as may be applicable to the specific installation is a continuous requirement for training supervisors.

b. Scheduling classes for nonmilitary-type security forces is often difficult. It is often impossible to assemble an entire security force or even a complete shift at any one time to participate. As a result, the supervisor of training must take care to provide an opportunity for each man to receive the training he needs.

9-12 Evaluation of Training

a. Using tests or examinations (FM 21-6) to evaluate performance is a necessary step in the training program. These tests, which may be oral, written, or a type of performance test, should be given at least once a year to determine that high standards of proficiency are achieved and maintained by the entire force. A testing program also aids in improving training by:

(1) Discovering gaps in learning.

(2) Emphasizing main points.

(3) Evaluating instructional methods.

b. Security training received by personnel at their units should be entered in unit training charts or records. This record helps to:

(1) Indicate individual degrees of skill.

(2) Establish priorities of instruction.

(3) Present a consolidated picture of the security force training status.

(4) Helps certify guard personnel.

9-13 Security Force Duties—MOS 95B10

Duties vary with the requirements of an installation, facility, or activity. Security forces achieve their purpose by a combination of actions consisting principally of those outlined here:

(1) Performs security foot, static, and motorized patrol.

(2) Detects violations of laws, regulations, and orders.

(3) Applies crime prevention measures.

(4) Searches suspects.

(5) Employs unarmed self-defense measures.

(6) Prepares military police security reports.

(7) Provides security for designated individuals, installation, and equipment.

(8) Employs intrusion detection sensors and devices.

(9) Controls entry and exits to facilities and vital areas.

(10) Deters pilferage, damage, and loss of supplies and equipment.

(11) Performs as a security guard during air movement operations and ground convoys .

(12) Participates in civil disturbance operations as a member of

(a) Crowd control formation
(b) Patrol of disturbed area
(c) Special reaction team(s).

(13) Employs civil disturbance munitions and equipment.

(14) Collects security police intelligence.

(15) Administers first aid.

(16) Employs individual and crew-served weapons.

(17) Operates radio equipment.

(18) Operates wheeled and tracked vehicles.

(19) Conducts rear area security operations and activities, as appropriate.

(20) Operates and enforces the system of personnel identification and movement control.

(21) Observes and patrols designated perimeters, areas, structures, and activities of security interest.

(22) Observes and patrols areas outside the perimeter, to include operation of listening posts, as necessary to provide security in depth against enemy attacks or terrorist/guerrilla acts

(23) Apprehends persons attempting or gaining unauthorized access to any portion of the installation or facility.

(24) Checks depositories, rooms, or buildings of security interest during other than normal working hours to determine that they are properly locked and are otherwise in order.

(25) Performs escort duties for materiel or designated persons when required.

(26) Enforces the established system of control over removal of property and documents or material of security interest from the installation or facility. It maybe necessary for security force personnel to establish the system and monitor its operation.

(27) Responds to protective alarm signals or other indications of suspicious activities.

(28) Acts as necessary in situations affecting the security of the installation or facility (including fires, accidents, internal disorders, and attempts to commit espionage, sabotage, or other criminal acts).

(29) Generally safeguards information, materials, or equipment against espionage, sabotage, unauthorized access, loss, theft, and damage.

(30) Operates and enforces regulatory traffic controls and procedures to aid in the smooth flow of traffic and to prevent or reduce the number of accidents.

(31) Performs such other security duties outside the installation or facility as may be required, such as port and harbor security, loading/unloading operations aboard ships, security escort on lines of communication, ambush/counterambush operations, and other duties required by the local situation.

(32) Reports periodically, as a matter of prescribed routine under normal conditions, and as necessary in unusual or emergency circumstances.

9-14 Security Force Duties—MOS 95B20

a. Leads security troops involving:

(1) Military police security patrol.

(2) Squad activities.

(3) Small security detachment/section operations and actions, plus rear area security operations and activities.

b. Assists in coordinating security activities with civil police organizations.

c. Assists in supervising the following:

(1) The crime prevention program.

(2) Security training.

(3) Participation in unit employment.

(4) Riot and crowd control operations on security installations.

d. Supervises military and civilian guards.

e. Helps conduct physical security surveys.

f. Inspects and posts military police security static post guards and motorized patrols.

g. Prepares reports, forms, and records on MP security operations and activities.

9-15 Security Force Duties— MOS 95B30

Leads military police security section or large squad and supervises a platoon with less than 40 positions.

a. Assists in:

(1) Planning

(2) Organizing

(3) Directing

(4) Supervising

(5) Training

(6) Coordinating

(7) Reporting activities of subordinate elements.

b. Supervises and directs receipt, storage, and distribution of:

(1) Weapons

(2) Ammunition

(3) Supplies

(4) Equipment, and

(5) Food to subordinate elements.

c. Directs execution of the unit's crime prevention program.

9-16 Security Force Duties— MOS 95B40

a. Leads military police security detachment or section of 40 or more positions or supervises and directs a platoon of 40 or more positions, and processes security operations and intelligence information.

b. Collects offensive and defensive security intelligence information for development of military police security operations.

c. Supervises and trains personnel in military police security operations and intelligence activities.

d. Monitors the unit's crime prevention program.

e. Assists in coordination and implementation of military police.

- Security operations
- Training programs
- Administrative matters, and
- Communication activities.

f. Assists in production and administration of

- Security staff journals
- Files, records, and security reports.

g. Assists in planning rear area security operations, as appropriate.

9-17 Security Force Duties— MOS 95B50

a. Supervises physical security duties of 95B50 security personnel.

b. Serves as principal noncommissioned officer in a military police physical security company.

c. Supervises the progress of security operations and intelligence information at battalion or higher level.

d. Interprets, supervises, and monitors execution of company administrative, logistical, maintenance, training, limited rear area security, and tactical policy and SOP.

e. Monitors and inspects duties performed by subordinate enlisted personnel.

f. Prepares security charts, reports, and related documents and material.

g. Plans the unit's crime prevention program.

9-18 Security Duties—Officer

a. Law Enforcement Officer (Security Platoon Leader) duties:

(1) Leads, supervises, directs, and monitors enlisted military police security guards and supervisors in the execution of assigned security duties.

(2) Helps insure that adequate security is provided to critical equipment, facilities, items, lines of communication, and government officials.

(3) Assists in planning and coordinating physical security surveys and inspections involving the unit's physical security mission.

(4) Assists in planning and implementing the unit's physical security operations and activities.

(5) Helps develop the unit's crime prevention program.

(6) Performs the duties of convoy security officer and participates in limited rear area security operations.

(7) Performs other logistical, administrative, maintenance, and training duties as assigned.

b. Law Enforcement Officer (Security Unit Commander) duties:

(1) Commands, directs, controls, and monitors unit military police physical security operations and functions.

(2) Directly insures that a safe and secure physical security environment is provided for sensitive and critical equipment, facilities, items, lines of communication, and government officials.

(3) Plans and monitors implementation of physical security surveys and inspections involving the unit's mission.

(4) Coordinates with supporting investigative units concerning illegal activities.

(5) Coordinates with local, US, and allied law enforcement agencies, as appropriate, to insure a total integrated security effort during routine and emergency operations.

(6) Coordinates with the local provost marshal to insure that local military police law enforcement support is performed in nonrestricted depot and installation areas.

(7) Insures that a unit crime prevention program is designed and implemented.

(8) Assists the security officer, when applicable, in preparation of security plans, policies, and SOPs, and performs the necessary security inspection of guards, equipment, alert procedures, and sensitive areas and facilities.

(9) Insures all unit personnel are properly trained for daily security operations and physical security inspections and technical security inspections by higher headquarters.

(10) Insures the unit is prepared to participate in limited rear area security operations as appropriate.

153-846 0 - 94 - 9

Recommended Qualifications For Law Enforcement Officer

- Completion of the Military Police Officer Advanced Course, or
- Appropriate subcourse of the Army Correspondence Course Program Military Police Officer Advanced Course, or
- Completion of resident physical security training at the US Army Military Police School/Training Center, or
- Equivalent training or experience.

c. Physical Security Officer (Manager) duties. If a depot/installation or activity is so configured by TDA that a separate security officer is assigned in addition to a security unit commander, the security officer performs the following duties:

(1) Responsible for continual review and update of the physical security plan.

(2) Conducts inspections of on-duty guard personnel, IDS equipment, SOPs, alert procedures, safety equipment, and sensitive areas and facilities.

(3) Coordinates continually with:

- FBI
- CID
- Local PM
- MI
- DAFE
- Local police
- State/county police.

d. Depot Security Officer duties:

(1) Performs liaison with:

- CID
- MI
- Local police
- Local PM
- FBI
- State/county police

(2) Responsible for development, implementation and supervision of:

(a) Depot access control.
(b) Material/vehicle control.
(c) ID/badge systems.
(d) Vehicle registration.
(e) Security clearance initiation on all depot employees.
(f) Security information programs.
(g) Accident/incident investigations.
(h) Traffic control–routine and special.
(i) Law enforcement and related functions.
(j) Conduct of physical security inspections.
(k) Security patrolling.
(l) Conduct of a depot security awareness program.
(m) Operational security.
(n) Computer security.
(o) Security guard/supervisor training.
(p) Security guard/supervisor weapons security.
(q) Guard communications equipment security.
(r) Security of vital areas.
(s) Screening employment applications.
(t) Contingency plans.

(3) Directly responsible for logistical, maintenance and administrative support, operational education and training of:

- Three 50-man guard force branches
- Intelligence/investigation branches.

9-19 Security Force Instructions

a. Will be in writing and made available to each guard.

b. They are normally in one of the following forms:

- General instructions
- Special instructions
- Temporary instructions.

c. Reviewed at least monthly.

d. Security force manual must be made available for required reading by each member and cover the following:

- Operating procedures
- Policy establishment
- Organization
- Authority
- Functions.

e. Periodic inspection and examination of each individual's degree of security, skill and knowledge must be exercised by each appropriate supervisor.

Supervision and Management — Section IV

9-20 Supervision

a. A security supervisor has the task of overseeing and directing the work and behavior of other members of the security force. Effective supervision requires a complete understanding of the principles of leadership and how to apply them so as to obtain maximum performance from members of his force.

b. The supervisor is called upon to think and act in terms of many different jobs. He is often responsible for the selection, induction, training, productivity, safety, morale, and advancement of the members of the force. He must understand these and all other employment aspects of his force.

c. To maintain an alert, presentable, and efficient security force, there must be constant and constructive supervision. Supervisors must be in evidence, and they must conduct themselves as models of neatness, fair play, efficiency, and loyalty. The morale and efficiency of a security force is a direct reflection of the quality of its supervision.

d. The ratio of supervisory personnel to security personnel should be determined by the individual characteristics of each installation. In small compact installations, the ratio may be higher than at very large installation.

(1) There must be sufficient supervision to enable the inspection of each post and patrol twice per shift, plus sufficient backup supervisory personnel to provide for sick and annual leave.

(2) It is also essential that supervisors be in contact with security headquarters to control emergencies that may arise.

(3) Specific duties of a supervisor include the inspection and briefing of the relief shift prior to its going on duty, and the inspection of posts, vehicles, and equipment during visits to posts and patrols.

9-21 Responsibilities To Management

a. The physical security supervisor is responsible to management for the development of a security-minded organization. This program is greatly enhanced by a well-organized security education program.

b. The role of the physical security supervisor puts him in a position of advising on the formulation of policies for the physical security of an installation. His goals should be the accomplishment of the assigned

mission at the lowest possible cost consistent with the commander's policy. It is well for all physical security planners to remember that anyone can provide adequate security with unlimited funds; however, this is not a realistic approach. There must be a constant endeavor to effect justifiable economy wherever possible without jeopardizing the physical security program.

9-22 Supervisor's Relationship To The Security Force

Supervisors should strive to create and maintain a loyal force with high morale. Following are some of the means by which this may be accomplished:

a. Proper training and supervision.

b. Direction of the security force in an objective business-like manner while exercising consideration for the personal welfare of security force members.

c. Application of basic principles of human relations. The effective supervisor must know that there will be individual differences among members of his security force. He should be guided by the principle that subordinates are motivated indifferent ways; ambition can be stirred or pride hurt by his regard, or lack of it, for their welfare and feelings. A good supervisor must understand the needs and desires of each member of his force. He is their representative and they should be made to feel that he is the one with whom they can talk and discuss their problems, on a personal basis.

d. A good supervisor develops depth in his security force so that continuity of operations is assured. He can develop depth by rotation of assignments, cross-training in varied duties, etc.

e. A good supervisor has the reputation of being honest, considerate, and willing to listen to both sides of a grievance. He must have knowledge of his job and the principles involved, and the ability to teach these principles to his subordinates. All of these qualities help greatly in building confidence among his personnel and securing their cooperation. Specific techniques for securing cooperation include the following:

(1) Each person should be made to feel his job is an important one.

(2) Each person should be given an opportunity to express his thoughts, likes, and interests to the supervisor.

(3) Supervision should be based on individual needs.

(4) Supervisors should recognize achievement. For example, a security man of the month program may be implemented, with appropriate reward for outstanding effort or achievement.

(5) Personnel may be recommended for advancement for outstanding effort or achievement.

(6) The supervisor should maintain an attitude of impartiality in dealing with his subordinates.

f. An effective supervisor develops good discipline by establishing rules that are just, complete, easy to administer, and easy to understand. If a supervisor needs to take corrective action involving his security force, it may only call for "setting a man straight," which is a recommended technique for supervisors to consider. Types of situations in which verbal corrective action should be considered are:

(1) When the deficiency is due to lack of knowledge or training. (This must be followed by appropriate training.)

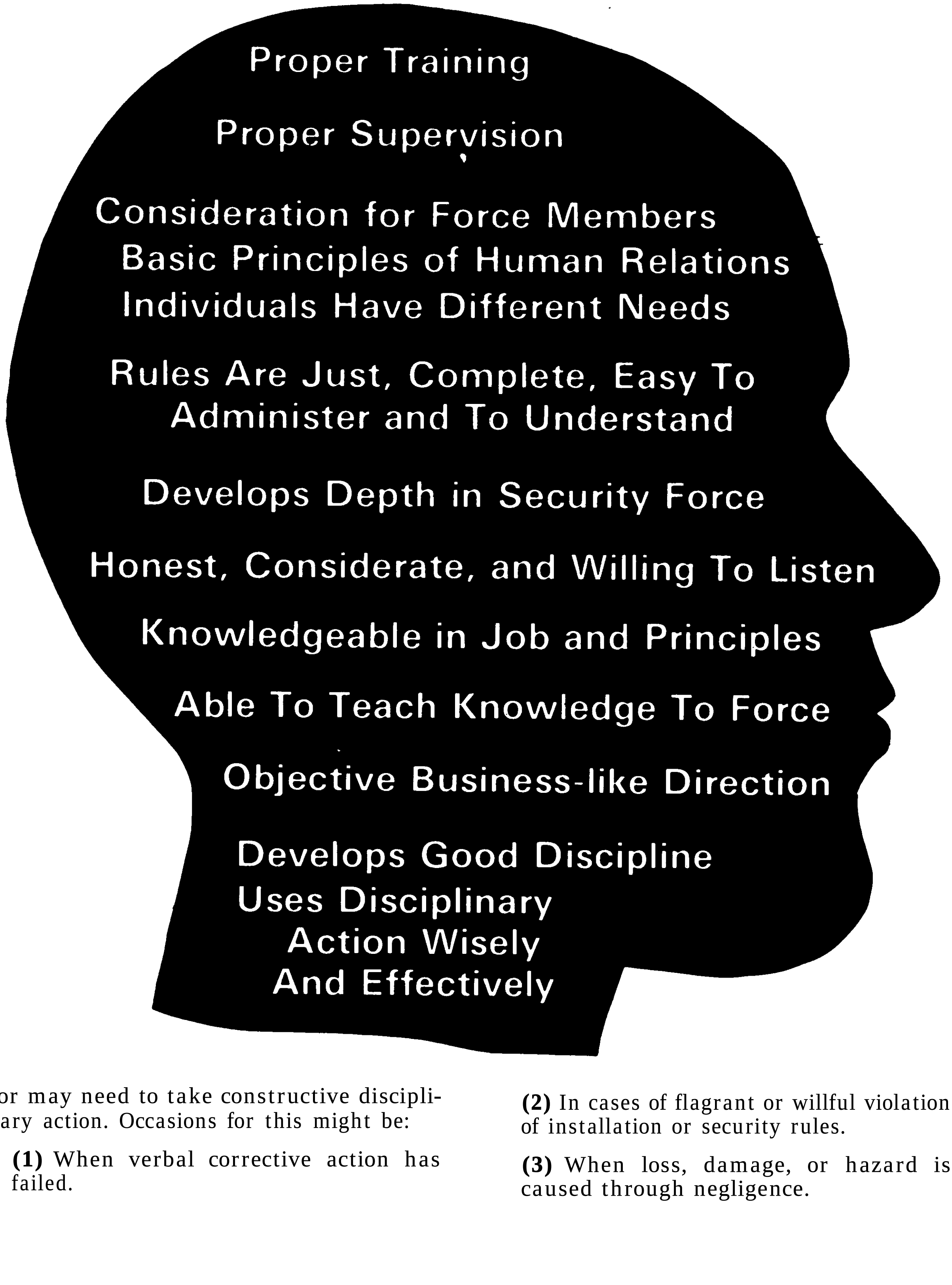
(2) When the error is trivial.

(3) When the action is a first offense.

(4) When it is due to old habits. (These must be corrected.)

g. Under some circumstances the supervi-

Profile of an Effective Supervisor



sor may need to take constructive disciplinary action. Occasions for this might be:

(1) When verbal corrective action has failed.

(2) In cases of flagrant or willful violation of installation or security rules.

(3) When loss, damage, or hazard is caused through negligence.

h. Disciplinary action should be handled calmly, in private surroundings, and the supervisor should have full knowledge of the facts. If punitive action is called for, the UCMJ, or pertinent civilian personnel regulations covering probation and discharge, should be consulted. It is well to remember that these are serious actions and should be taken only when all other measures have failed. The supervisor should bear in mind the requirements for documented proof of events and actions leading to the necessity for disciplinary action. When the decision has been reached as to the propriety of probation or reprimand, further action should be pursued vigorously and without fear of reprisal or seemingly excessive administrative burden. (For further discussion on military leadership principles, see FM 22-100.)

9-23 Supplements To Personal Supervision

Various means and devices may be successfully used as supplements to personal supervision or, in the case of small installations or remote areas, to supplant personal supervision as a means of assuring that necessary areas are patrolled and other functions performed. These include the following:

a. Recorded tour systems, under which personnel record their patrols or presence at strategic points throughout an installation by use of portable watch clocks, central watch clock stations, or other similar devices. These are effective means of insuring that such points are regularly covered, and have application at most installations and facilities. This system provides an after-the-fact type of supervision.

b. Supervisory tour systems by which a signal is transmitted to a manned central headquarters at the time the tour station is visited. These have application at a limited number of installations to supplement personal supervision, or to supplant personal supervision at installations with small security forces. These systems provide instantaneous supervision, plus a means of detecting interferences with normal security activities and initiating an investigation or other appropriate action.

c. All personnel on security duty should be required to report periodically to headquarters by the usual means of communication. The frequency of such reports will vary, depending on a number of factors, including the importance of the installation. Regularity should be avoided, to preclude setting a pattern by which an intruder can gauge an appropriate time for entrance.

9-24 Security Force Problems

a. Assignment to a unit with physical security functions is not always looked upon with favor by military police, many of whom prefer serving with a unit having broad general MP functions or requirements.

b. The nature of security force operations poses some morale problems that do not normally confront other personnel. The security force is required to be effective at all times, regardless of the weather, day, and hour. This necessitates duty hours on weekends, holidays, and night—hours usually considered nonduty time. These circumstances produce problems in living for both the individual and his family, problems that tend to lessen enthusiasm for the job. There is a direct relation between quality of performance and morale that forces consideration of these problems. The problem can be minimized by implementation of the following steps:

(1) Maintain high standards of discipline.

(2) Promote an aggressive security education program to insure that each man clearly understands the importance of his job. Each man must be made to understand the consequence of any breach of protective barriers. Each man should understand

that the human element in security operations makes the difference between success and failure.

(3) Arrange shifts so that personnel periodically have a 48-hour period free from shift requirements.

(4) Consider shift rotation as one solution to boredom. However, there are advantages and disadvantages to be considered on the question of rotation of individuals from shift to shift. An advantage of permanent shift assignment is that each shift presents its own problems in security, and if the man is permanently assigned he is able to learn these peculiarities and is able to cope with them more efficiently. Another advantage of regular assignment to the same shift is that the physical welfare of the man requires that he work regular hours and establish regular habits of eating and sleeping. The major disadvantage of being permanently assigned to one shift is that some shifts are considered very undesirable from the standpoint of hours of work, and if assignments are made permanent, the same personnel will be working the same undesirable hours.

(5) The transfer of a man from one shift to another could be considered a reward, since the working hours of some shifts are more desirable than others. For better operation, the integrity of the shift should be maintained as a unit. In this way, each man learns the abilities and limitations of the others, and is able to function much more efficiently as a member of a coordinated team.

(6) Establish good recreational facilities at appropriate locations along with an organized athletic program, as this helps considerably in the development of loyalty, pride, and enthusiasm for the unit or installation.

(7) When practicable, hot food should be provided to men going on post and those coming off, as this is a definite morale factor.

c. If both military and civilian security forces are used at an installation or activity, the provost marshal or physical security manager should insure equality of treatment for members of the entire force. Any instructions or corrective action should be passed to appropriate supervisors for dissemination to the security force.

d. At installations or facilities where security force personnel are posted at exits/ entrances or at other internal posts to control the movement of traffic, they do not merely stand guard. Such personnel check transportation movement documentation against actual loads on trucks. They check for hidden contraband, pilfered property or goods, authorization for access onto or within the facility/installation, and safety violations. They conduct searches and seizures when authorized, and enforce regulations and assist visitors, as appropriate. People engaged in the performance of worthwhile duties do not become bored. When personnel are required to either stand or walk post merely as guards, especially in an oversea environment, they must be checked frequently for alertness.This requires aggressive and imaginative supervision, vulnerability tests, greater frequency in change of shifts, and even the rotation of personnel from one post to another within shifts to combat boredom created by unchallenging duties.

e. Continuous endeavors should be made by physical security supervisors to provide the best conditions possible and to maintain an aggressive program to develop a high state of morale and esprit de corps among security force members.

9-25 Uniforms

a. All security force personnel should be required to wear the complete prescribed uniform as outlined in AR 670-10

(for civilian personnel), AR 670-5, and FM 19-5 for military police and other security personnel. Deviations from the prescribed uniform requirements should not be made except for such additional items of wear as are necessary to protect the health, comfort, and safety of the individual.

b. The duty uniform should be worn during all tours of duty. Normally, it may be worn during off-duty hours only between the place of residence and place of duty.

c. Each member of the security force should maintain high standards of personal and uniform appearance, and should wear a neat, clean, and well-pressed uniform.

9-26 Vehicles

The security force should be furnished with sufficient vehicles to maintain patrol standards established by the installation commander. Vehicles assigned to the force should be equipped with two-way radios to obtain the greatest possible use of all personnel and vehicles. Vehicles should be marked as prescribed in AR 746-1.

9-27 Firearms

a. Weapons. Security force personnel should be appropriately armed at all times while on duty. Normally, the weapon of issue to civilians will be either the revolver, cal. 38, or pistol, cal. 45. However, the commander may prescribe other weapons for the security force, based on need and requirements. Weapons normally are loaded with live ammunition, except where prohibited for safety reasons. The use of privately owned weapons while on duty should not be authorized. Weapons and ammunition issued to security force personnel should not be removed from the installation except in the course of official duty (and then only when authorized by proper authority). When not in use, weapons must be secured in arms racks or storage rooms as prescribed by AR 190-11.

b. Control of weapons used by security force personnel on duty must comply with AR 190-11. Procedures should be established for the control and accountability of weapons at all times.

c. Inspection of weapons should be conducted at the beginning and end of each tour of duty, and at such other times as necessary to insure proper maintenance and to determine if the weapon has been discharged. A written report should be prepared and filed on the discharge of any weapon except for authorized and supervised training. Such report should be prepared by the individual to whom the weapon was issued at the time it was discharged. Appropriate action should be taken in those instances when it is determined that the discharge of a weapon was not in the performance of assigned duties, or when it was the result of negligence.

d. Weapons for emergency use. In addition to the use of individual weapons, security force personnel should be furnished weapons as needed to sustain the security force in the event of an emergency, riot, or other disturbance. Weapons in this category should be properly secured as indicated above, maintained at strategic points, and kept in readiness for issue when appropriate.

e. Ammunition supplies for security force use must be maintained in secured storage containers, as outlined for weapons, to prevent unauthorized access. Ammunition must be issued only under proper supervision for authorized purposes. Ammunition issued to members of the security force for any purpose must be accounted for by individual members immediately upon completion of the period or purpose for which issued. Any ammunition unaccounted for will be the subject of a report of its disposition by the

individual in the same manner as for weapons (a, preceding page).

9-28 Signal Items

The security force should be equipped with radio transmitters/receivers, both vehicle-mounted and portable, and telephones for expeditious transmission of reports and instructions between security headquarters, posts, and patrols. This equip ment is considered essential for the efficient operation of the security force and the accomplishment of its assigned mission. Proper use and care by security personnel will enhance equipment usefulness and capability.

9-29 Miscellaneous Equipment

Security managers or supervisors should obtain such other equipment as may be necessary to implement their security program. Items in this category may include, but are not limited to, warning lights, sirens, and spotlights for vehicles, portable lights, flashlights, first aid kits; traffic control devices; and items of wear for the health, comfort, or safety of security personnel.

9-30 Vulnerability Tests

a. Because of the routine, repetitious nature and solitude of many security requirements, personnel must make special efforts to overcome a tendency to relax in their performance of duties. To check on this weakness and keep personnel aware of their responsibilities, and as a means of pointing out other weaknesses in the security system, vulnerability tests may be used. These tests are normally designed by the provost marshal or the physical security manager, and consists of attempts to breach security in one way or another, such as entering or attempting to enter a restricted area through deception. The types of deception which may be used are almost unlimited.

b. Test Objectives:

(1) A vulnerability test provides the commander an estimate of the vulnerability of his installation or facility; tests the effectiveness of the security force and other personnel; alerts personnel to the techniques that could be used by an intruder; and provides material for corrective instruction.

(2) Specifically the test should examine:

(a) Improper enforcement of identification and control procedures by security personnel, such as failure to:

- Determine authority for entry.
- Scrutinize identification media. The ways of using fake credentials to deceive security forces are numerous. The only way to detect such trickery is to know the details of each type of access credentials and to examine them thoroughly. Security tests and inspections have indicated that unauthorized persons have been granted access to restricted areas by altering or forging passes, by faking identification by telephone, and by playing upon the sympathy of security personnel with excuses.
- Ascertain identity.
- Detain unauthorized persons.
- Conduct immediate preliminary search of suspects.
- Enforce security procedures.
- Report security violations.

(b) Susceptibility or gullibility of security personnel to plausible stories by intruders or members of the security force and other personnel of the installation. This inclination to believe, on slight evidence, an individual who may be attempting to gain unauthorized access to a restricted area is the product of two factors: monotony, and a desire to save time. In the busy activity of individuals who are authorized access to

a restricted area, it is easy for security personnel to be deceived by slight evidence. The monotony of verifying hundreds of access credentials which are valid can dull the sensitivity to detect one which is invalid. Many attempts to deceive security personnel involve false credentials, assumed rank, or falsely marked vehicles.

(c) Unauthorized disclosure of information by members of the security force and other personnel of the installation.

c. Test Planning and Preparation. Detailed planning and preparation is a requirement for effective testing of security. Planning should include the following:

(1) Plan in secrecy to avoid alerting installation personnel. Prior knowledge by the security forces or other people produces invalid test results and thus defeats the purpose of the test.

(2) Establish a priority of targets that seem more vulnerable than others. Do not test the same target on a continous basis. Attempt to test all eligible targets over a time. This will keep all personnel alert, rather than those of only one area.

(3) Select qualified people to conduct vulnerability tests. Criteria for personnel should include:

(a) Appropriate security clearances for all members of the team at the same or higher classification level of the area or installation that might be entered. Such clearances preclude any compromise of security interests if a safe is found open or an area containing classified matter is entered.

(b) Members of the test team should be unknown to members of the security force or other personnel of the installation or facility.

(c) Team members should be capable of quick thinking to adapt to their cover stories.

(d) Members should be able to bluff in a convincing manner.

(e) The cover story should originate with the provost marshal or physical security manager. A well-contrived cover story is necessary. It should sound convincing to provide an adequate test of the security force.

(4) Obtain appropriate material for testing. This may include:

(a) Clothing appropriate to assumed identity.

(b) Props necessary to support cover story.

(c) Tools appropriate to assumed identity, such as repairman or plumber.

(d) Transportation.

(e) False or altered credentials.

(f) Simulated sabotage devices (explosives, incendiaries, abrasives, corrosive acids, etc.) to provide realism. These should meet the following criteria:

- The device should be suitable for the target.
- Device should be the same size and weight as the genuine article.
- The device should be properly labeled as the device which it is simulating.
- Simulated time of detonation should be indicated on the device to simulate realism. There is always the possibility y that the device will be discovered before the simulated time of detonation.
- Planting of the device should be related to the type of device used. It should be placed to simulate the greatest amount of destruction or to achieve the desired results.

d. Test Instructions.

(1) The officer in charge of the test should select the method or techniques to be used based on the ability of testing personnel and supporting materials available.

(2) This officer should provide for flexibility in selection of targets. His orientation to team members should include the following instruction:

■ Exploit any security weakness that becomes evident during the test.

Remember the Test Objectives:

- ☐ Estimate vulnerability for commander
- ☐ Determine effectiveness of security force and other personnel
- ☐ Alert guard force and commander to techniques that could be used to attempt a security breach
- ☐ Provide information for corrective action

- Change tactics or take evasive action as necessary.
- Strike targets of opportunity.

(3) Personnel assigned to conduct vulnerability tests should be given only such information concerning the installation or facility that an outsider would normally have or could obtain through reasonable efforts.

e. Test Safety. Instructions to test team members should also include safety precautions. **Test personnel should not:**

(1) Scale barriers of any kind, because the guards may have instructions to fire.

(2) Forcibly resist apprehension, because of the danger involved. By resisting apprehension, personnel will nullify benefits to be achieved.

(3) Use dangerous materials that might cause harm to any person involved directly or indirectly.

(4) Use any action that might influence normal operations or safety or equipment of the installation.

f. Techniques for Infiltration of Security Areas. Personnel conducting vulnerability tests should consider the following techniques for infiltration of security areas:

(1) Entry through unguarded gates or open areas not under observation by security forces or other personnel.

(2) Use of false or altered passes or badges through active gates manned by security personnel who give only a cursory glance at these credentials.

(3) Entry through areas without presentation of identification media.

(a) One method is to bypass security forces by mingling with a work group entering the area.

(b) Another method is to obtain permission to enter the area, claiming loss of identification media and using a plausible story.

(c) A third method involves deception by false representation, whereby a member of the vulnerability test team poses as a high-ranking officer or civilian dignitary, or as a repairman, installer of equipment, inspector, etc., who would have legitimate business in the area.

g. Neutralization of Escorts. After making successful entrance to a security

area, testers must in many cases, neutralize an assigned escort to accomplish the test mission. Procedures for this include the following:

(1) When operating as a team, use ruses to divert the escort's attention.

(2) Request use of latrine and leave if not accompanied by escorts.

(3) Devise any other means as opportunities present themselves. However, no force should be used to overpower the escort.

h. Planting Simulated Sabotage Devices. Procedures to follow for planting simulated devices include the following:

(1) The device should be planted as appropriate if access can be gained, in the location where it would do the most damage.

(2) Place on any vehicle entering the area.

(3) The device can be given to authorized personnel entering the area by using bribery or coercion, or by secreting it in their clothing or accessories such as purses or briefcases.

(4) Mail the device to a person or activity in the security area. Estimated time of delivery can be obtained by surveillance of delivery personnel.

i. Review and Analysis of Vulnerability Tests.

(1) Upon completion of vulnerability tests, results should be reported, preferably in writing. The report should be carefully reviewed and analyzed by the provost marshal, physical security manager, and others responsible for physical security planning. The review and analysis should provide an evaluation of the physical security program and serve as a basis or guide for effecting necessary changes.

(2) Review and analysis of the method and procedures used for vulnerability tests provide guidance for future tests.

(3) Test results should be given appropriate security classification (should be the same as or higher than the security classification of the area). Dissemination of test results should be rigidly controlled and limited to those who have the required security clearance and a need to know.

9-31 Sentry Dogs

The requirements for physical protection of installations or facilities within the United States and oversea theaters of operations continue to increase, yet the manpower available for this purpose has always been, and probably will continue to be, limited. The sentry dog, properly trained and properly used, can be a great asset to the physical security program of some installations or facilities and should be considered in developing an effective crime prevention program. Use of the dog and posting of conspicuous signs has been found to be a strong psychological deterrent to attempted intrusion.

a. Mission of the sentry dog is to detect intruders; alert his handler; and when necessary, pursue, attack, and hold any intruder who tries to escape. Normally, the dog has done his job when he detects the intruder and alerts his handler. The handler is then responsible for taking appropriate action.

b. The sentry dog and handler work as a team. Since the outstanding qualifications of the sentry dog for security type duties are his keen sense of hearing and smell, he is used to most advantage in darkness or poor visibility when human vision is restricted. Because of the added perception of the handler-dog patrol, patrol routes can often be lengthened without sacrificing coverage. (FM 19-35 presents detailed discussion on types of dogs; their desirable characteristics; traits and care of military dogs; basic training; and specialized training.)

c. For this manual, only the sentry dog will be considered. There are, however, situations in which the use of sentry dogs is undesirable or impractical due to their limitations (paragraph i, below). In such situations the use of other types of dogs (FM 19-35) should be considered.

d. The sentry dog is used on exterior or interior security duty as a watchdog. This type of dog is trained to give warning to his handler by growling or barking, or by silent alert. He is always worked on a leash. The handler can depend on the dog to alert him to the approach or presence of strangers in or about the area being protected. When the dog alerts, the handler must be prepared to cope with the situation as circumstances dictate. That is, he must challenge, investigate, remain concealed, or make an apprehension. The dog, being kept on leash and close to the handler, also helps as a psychological factor in such circumstances. He will attack upon being released from the leash.

e. Sentry dog posts and patrols can be broken down into three types for reference and use. These are:

(1) Perimeter. This type patrol is along a portion of, or the entire fence line, inside or outside, which may enclose security areas such as tactical aircraft parking areas, POL storage areas, POL pipeline. and pumping stations, remote transmitter sites, guided missile sites, radar sites, special weapons and ammunition storage areas, and depot storage areas.

(2) Area. This type post is located around a group of buildings, or at such places as launching pads that may be considered critical, but do not justify perimeter posts. These posts are used for security in depth.

(3) Specific. Buildings such as warehouses or offices which contain valuable or highly classified materials.

f. The sentry dog patrol is especially effective in areas of little activity such as isolated perimeters, remote storage areas, pipelines, and open storage areas. The dog also tends to keep the man on post more alert, give him added self-assurance, and to relieve the ever-present monotony and loneliness of security duty.

g. In addition to a man and dog walking post, which is the most common and desired method, there are other methods of employment of dogs. Some of these are:

(1) Sentry dogs may be used as warehouse dogs. Dogs may be placed in warehouses at the close of the day, remain throughout the night, and then be taken out of the warehouse the next morning. This eliminates the necessity of having a guard stay with the dog all through the night, only requiring a roving patrol to check on the presence of the dog. The dog will alert the security force by barking at any attempt by intruders to enter his patrol area.

(2) These dogs also may be used on cables which may be extended between two buildings or areas. The dog is hooked to this cable and permitted to run its length.

(3) Sentry dogs also may be used between double fenced areas used primarily around exclusion areas. In this situation the dog is allowed to run between a double fenced area that is blocked off every 400 to 500 yards. The sentry dog will alert his handler if anyone comes near the fence, inside or outside.

(4) Such dogs also may be posted in front of entrances to a security area and will bark when anyone comes close.

(5) Sentry dogs also may be used in vehicles. While this method has not been used to any great extent, it has possibilities for security force applications.

h. Proper use of the sentry dog depends upon the existing situation and results desired; but normally the handler/dog patrol is the most effective method of employment. Regardless of how the sentry dog is used, the mere knowledge by potential intruders that dogs are on duty in the area has a

great psychological effect and often is a deterrent in itself. A vicious dog is often more feared by intruders than an armed guard.

i. The sentry dog is a very versatile animal; however, he does have some limitations with respect to type of assignment. The odor of petroleum products decreases the effectiveness of his sense of smell. Noise is a definite limitation, as it decreases his sense of hearing. Activity near a sentry dog post is also another limitation, as it tends to distract the dog.

j. Advantages of Sentry Dogs:

(1) Presence of sentry dogs provide a very strong psychological deterrent to intruders.

(2) Use of dogs is beneficial where security forces have been reduced.

(3) The dog's keen sense of smell and hearing enable him to detect the presence of danger and to alert his handler.

(4) Safety is a consideration. There is less chance of a fatality through the release of a dog than through firing a weapon at an intruder.

(5) The dog's ability to detect/apprehend intruders during hours of darkness is a definite advantage.

(6) A dog is more effective than a man during inclement weather. This type of weather offers ideal conditions for illegal entry.

k. Disadvantages of Sentry Dogs:

(1) Attrition and turnover of personnel trained as handlers reduces the efficiency of the dog program.

(2) A break-in period is necessary to facilitate man and dog working as a team. This results in many nonproductive hours.

(3) The type of dog best suited for security work is naturally dangerous. Care must be taken that innocent persons are not hurt by the dogs.

(4) Kennels and training areas must be isolated and kept off limits to unauthorized persons. Signs should be posted warning of the presence of sentry dogs. In oversea areas, these signs should be bilingual.

(5) Care and maintenance of sentry dogs must be considered in manpower requirements. To maintain the physical fitness required of sentry dogs, periodic services of a veterinarian are necessary. This often poses a problem at small or isolated installations or facilities. Special facilities are required for care and training of sentry dogs, which adds to the initial expense of adding dogs to the security program.

(6) The selection and training of handler personnel must be carefully accomplished. The qualities of a handler dictate, to a great extent, the effectiveness of the sentry dog. Volunteers and persons who like and understand dogs are not always available as handlers. There will be some morale problem among the handlers as most of the work is at night and, in addition to security duty, they are normally required to care for and train their assigned dogs.

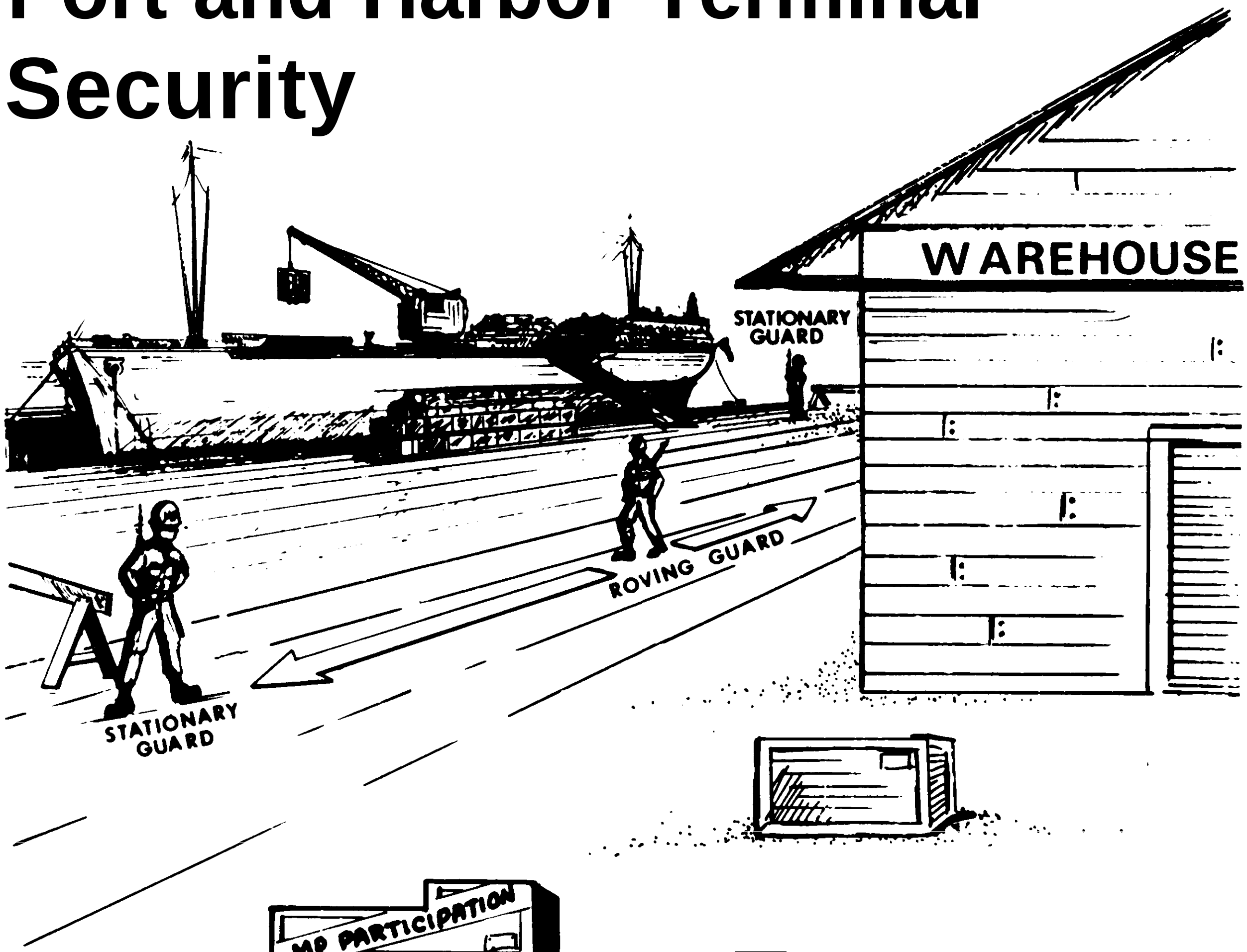
(7) Public relations must be considered when planning for the use of dogs. There is strong feeling on the part of many persons that using dogs for security or police purposes is uncivilized.

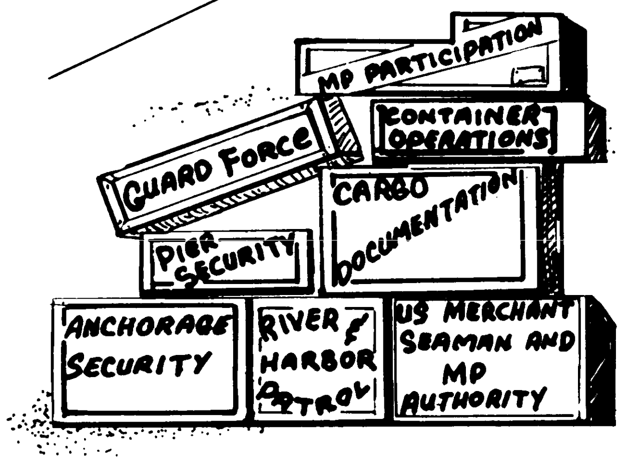
(8) Although these problem areas must be considered, care should be exercised that the value of the sentry dog, especially in a theater of operations, is not underestimated. Any method of reinforcing available manpower, whether it be weapon, machine, or animal should be carefully appraised. Certainly the capabilities of a man will increase in scope when augmented by a properly trained sentry dog. The sentry dog, used with other physical safeguards, can be invaluable to the commander's physical security program.

(9) AR 190-12 provides additional detailed guidance on all aspects of the sentry dog program.

Chapter 10

Port and Harbor Terminal Security





Theft and pilferage of cargo are extremely serious problems in terminal operations. A seemingly insignificant bit of laxness insecurity operations and procedures may provide a clever thief an opening to steal as much as a loaded container.

Physical protection requirements are the same in terminal areas as in warehouse and open storage areas. The need for personnel identification and control is, if anything,

greater. Many of the problems encountered or physical security procedures and techniques used in storage and intransit security (ARs 190-11, 50-5) are equally applicable in terminals.

There are, however, some different and frequently more demanding aspects of physical security due to the very nature of a terminal. The exposure to pilferage and sabotage is intensified and broadened because ports and harbors are prime targets for enemy and criminal activities, plus the perimeter areas of these activities are more vulnerable because of extensive distance and exposed beach or pier areas.

Terminal areas may include modem piers and warehouses, or may be an unimproved beach on which logistics-over-the-short (LOTS) or roll-on/roll-off (RORO) operations are conducted. The water-side may be anything from a broad and deep harbor to a narrow and shallow river, either of which may be under constant or intermittent enemy attack, either open or covert. All of these elements contribute to problems especially attendant to physical security of terminals.

Frequently Overlooked Functions — Section I

10-1 Military Police Participation

a. There are three important functions in terminal operations in which the physical security aspects are frequently overlooked and military police participation is not always sought. Provost marshals and military police commanders should be particularly aware of these functions, and should seek out all opportunities to participate in them. They are ship destination meetings, boarding parties, and reconnaissance and site selection in LOTS operations.

(1) Ship destination meetings. Ships, especially those en route to a theater of operations, usually sail from their ports of origin with only a tentative destination, since it is not always possible to determine the most desirable point of discharge until the ship arrives in the theater. The final destination is determined at a ship's destination meeting conducted by the appropriate commander. Many factors that must be considered in this determination include characteristics of the:

- Ship.
- Ship's cargo.
- Capabilities of the terminal.
- Capabilities of the land transportation system.

(a) Military police interest includes advance determination and planning for the provision of MP support required during unloading/debarkation operations while the ship is in port.

(b) A most important item for determination at this time is the nature of the cargo-whether it is dangerous or hazardous, sensitive, or highly susceptible to pilferage. This information should be used to determine the amount and types of MP support required, and for briefing all persons assigned.

(2) Boarding parties. When the ship's manifest and cargo disposition instructions have been received, plans are made for unloading. Before any movement or

unloading begins, a boarding party goes aboard to inspect the cargo and its manner of stowage, and to check on troop units or individuals to be debarked. This boarding party is normally led by the terminal operations officer. A military police representative should be included, to obtain information necessary for planning for MP support (such as hatch and/or deck guards, patrol boat escorts for lighters, etc.) and to observe, or receive reports on, any indications of pilferage or sabotage of cargo en route.

(3) Reconnaissance and site selection in LOTS operations. Logistics-over-the-shore (LOTS) operations require selection of suitable sites, based initially on a study of maps and hydrographic charts and analysis of aerial reconnaissance reports by the terminal group or brigade commander.

(a) Final determination is based on detailed ground and water reconnaissance by representatives of the engineer, signal, amphibious and landing craft units, and others as required.

(b) Military police representation should be included in these meetings and functions to determine the support need for:

- Traffic control operations
- Security of the pier and dock
- Beach security
- Convoy escorts and route selection
- Other MP activities.

b. Another activity in which the military police should be represented is the daily review of ships in port and en route. (This review may be conducted as a part of the ship's destination meeting, or it may be separate.)

(1) Progress in unloading/loading of each ship is reviewed so that an estimate can be made of clearance of a ship from the port and its replacement by another.

(2) Reviews may also be made of any factors that would affect plans previously made at ship's destination meetings, such as the necessity to reschedule a ship due to the nature of its cargo, delay en route, or similar factors. All such reviews will provide information essential to the provision of adequate military police support.

Responsibilities and Functions — Section II

10-2 Who's Responsible

a. The entire responsibility for a US Army terminal is that of the transportation terminal commander. He is responsible for:

- Safety and security of the entire terminal.
- Personnel assigned to, passing through, or working within the terminal.
- Security of all cargo from time of arrival in terminal to departure, either inbound or outbound.

b. The **provost marshal, military police commander,** or **military police physical security staff officer,** assigned or attached to the terminal advises, recommends, and assists in preparation of physical security plans and implementing directives. He also either commands or supervises security guard forces assigned to the terminal

(military and civilian), and participates in the coordination of all security and defense activities of the terminal (tactical and nontactical).

10-3 Terminal Areas Defined

A terminal is composed of a number of distinct, although correlated, areas, such as storage areas (covered and open), piers (land and water sides), beach or shore areas, entrances/exits, anchorage areas, and ships tied up at piers. It may also include POL discharge points, pipelines, and POL storage areas.

10-4 Water Terminal Guard Force

The guard force is the key to successful security.

a. Guard posts are motorized, stationary, or walking, depending on the type of supplies and cargo on the wharves, types of ships, and location and nature of the posts.

b. Gate guards check passes and badges of all individuals entering or leaving the terminal facilities; issue and check badges of authorized persons entering or leaving restricted areas in the terminal, such as piers, wharf sheds, vessels, and ammunition areas; search bundles and packages being taken from the area; examine trip tickets and documentation of cargo vehicles; control vehicle, railroad, and pedestrian traffic; and direct persons without proper passes to the identification section.

c. Pier and beach guards may be assigned to stationary posts to guard certain cargo areas, or they may be assigned to walking posts.

d. Pier guards check passes and/or badges, observe longshoremen, keep on the alert for evidence of pilferage or tampering, and assist or relieve other guards. Pier guards watch for small boats approaching the wharves. They check for proper identification of persons on board who desire to enter the pier or to board any vessel docked at the pier. These guards should have ready access to firefighting equipment and should maintain constant vigilance for fires under piers and heavy accumulations of oil next to pilings. They should not, however, fight fires at the expense of their security duties, but take only emergency measures while awaiting firefighting crews. Fires are sometimes started to distract security personnel.

e. Offshore guards, on stationary or walking posts, cover the harbor or stream end of wharves. They watch for trespassers in boats. They notify the officer of the day or the sergeant of the guard of the approach or a cargo vessel so that gangplank and ship guards will be on hand when the vessel docks.

f. Gangplank guards control longshoremen, terminal personnel, crew, and ship handlers boarding and leaving a vessel.

g. Hatch guards are posted as required in cargo hatches where longshoremen load or unload cargo. Requirement is based on the nature, value, or sensitivity of the cargo.

(1) Hatch guards stay on the same level as workmen, when possible, and report on damaged cargo and evidence of pilferage and sabotage. They must be alert for any attempts to divert, or “frustrate” cargo by changing destination markings. Damaged cargo must beset aside and guarded until it can be delivered to the terminal recooperage section for repair.

(2) Hatch guards must also coordinate with guards on deck to prevent dropping of cargo over the side of the ship.

10-5 Pier Security

The landward side of a pier can be protected by fencing and pass control; but the part of the pier that protrudes over the water cannot be protected in this manner. Not only is this part of the pier accessible from the sides and end, but also from the underside. Methods for securing the pier along its water boundaries are as follows:

- Patrols
- Protective lighting
- Booms
- Nets.

a. Patrols in small boats should be used in pier areas to prevent unauthorized small craft from operating in adjacent waters and to recover jettisoned cargo (figure 69).

(1) Patrol boats should be sufficiently narrow of beam to enable passage between the pilings when inspecting the underside of piers.

(2) Patrols walking along the end of the pier may be used separately or with boat patrols.

(3) All patrols should observe all debris floating on the water, as floating mines are sometimes delivered in this manner.

b. Protective lighting in the working area of piers should be adapted to construction and work needs. Slips and underpier areas should be lighted sufficiently to give night protection. Lights under a pier can usually be affixed to pilings close to the pier flooring. Wiring and fixtures in this area should be waterproof to insure safety in case of unusually high tides (chapter 6).

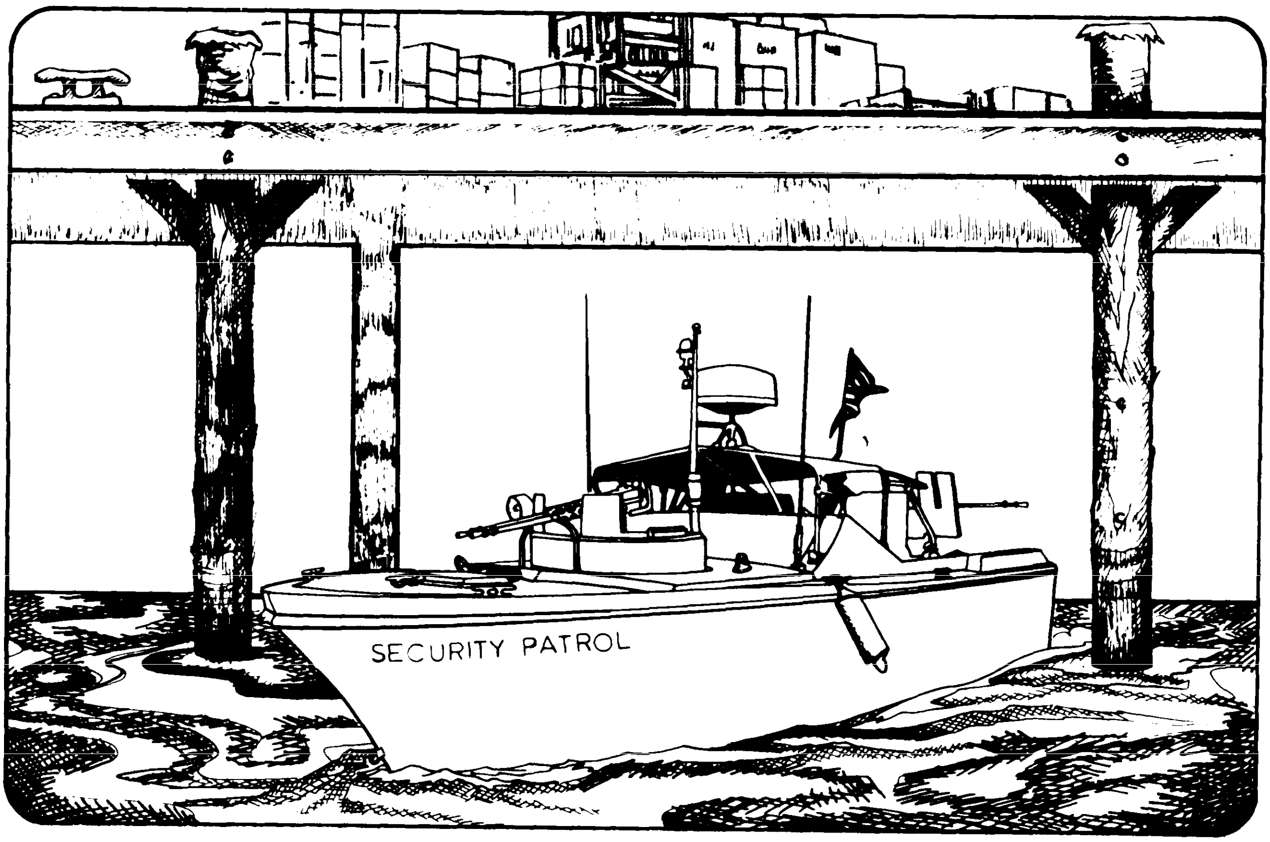


Figure 69—Pier security patrol boats should be able to move between pilings.

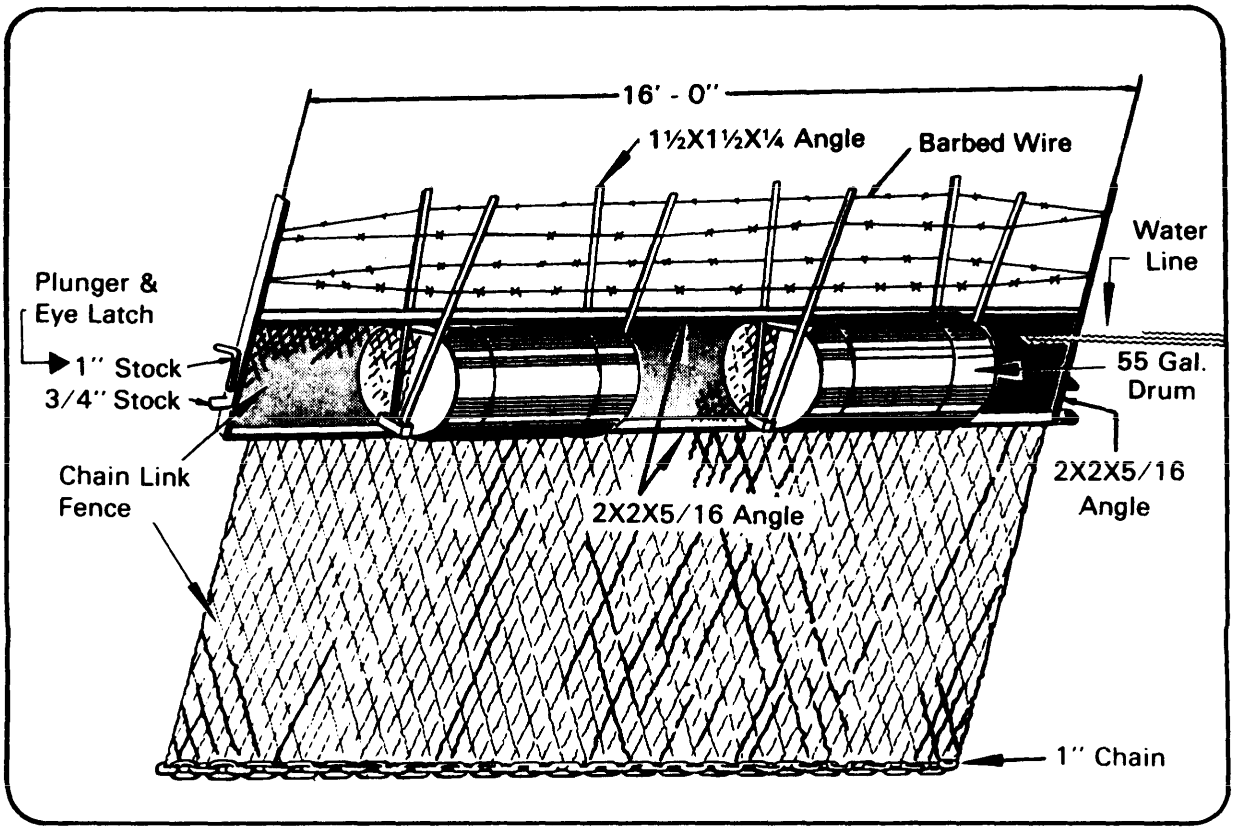


Figure 70—Example of boom and cable net protection.

c. Booms. Under certain circumstances it may be advisable to close off the waterside of a pier area by the use of booms (figure 70). A floating boom will prevent entry of small boats. To deny underwater access, a cable net must be suspended from the boom. An adaptation of the barrier described in chapter 5 may be used.

10-6 US Merchant Seamen And MP Authority

a. US civilians manning ships directly operated by a US agency, or any US civilian employed by a private business firm (foreign or US) under contract to one of the military department to support military operations in an oversea area are usually classified as Category I civilians.

b. Category I civilians are subject to US military police authority.

c. US military police exercise apprehension and detention authority over Category I civilians. Military police exercise this authority on a US Government installation or on US-controlled property or in combat areas and facilities under US control for offenses committed thereon or for protection of human life or property.

d. US-operated ports are considered facilities under US control. This includes vessels moored or anchored.

e. US military police are authorized to board a US Flag vessel to protect American citizens, US property or the US Flag vessel itself, whenever requested to do so by the master and in such other emergencies when

deemed necessary by appropriate lawful military authority. This police authority extends to US Flag ships at anchor, moored, moored by buoys, or at piers within pre scribed distance (usually the three mile territorial limits) of the host nation.

10-7 Cargo Documentation

a. Cargo moving through terminals is documented in accordance with DOD Regulation 4500.32-R. The basic document used is the Transportation Control and Movement Document (TCMD), DD Form 1384. (See appendix T for details.) This form is a seven-part, pre-numbered document which is initiated by the shipper for each shipment, for example, a truckload.

(1) The form shows the cargo (type, number of packages, etc.), the consignee to whom it is being delivered, names of the cargo checker and truck driver, and the time the cargo left the shipping point.

(2) Its purpose is to insure accurate and quick delivery of the cargo, reducing the risk of loss, theft, or pilferage.

b. The MP or physical security guard is concerned with the TCMD, since he must check this document against the load on a truck leaving the terminal, unless the load is sealed and wired or locked, such as a van or CONEX container. Otherwise, he must check the itemized TCMD, verify the types and number of packages, and check the security of the load in accordance with local requirements.

(1) If all is in order, he writes his name and organization on the TCMD, and stamps it with a date/time stamp, all in the spaces provided. He also records the date, time, and TCMD number in the gate log, and returns the TCMD to the driver.

(2) If he does not find all in order (for example, less packages than listed on the TCMD or load security requirements not met), he must hold the vehicle and report the circumstances immediately so that an investigation can be made and discrepancies corrected. He should know and be able to verify by a signature on the TCMD, the person(s) authorized to release the cargo. Signature cards or coded templates maybe used for this purpose.

c. Another instance of military police concern with the TCMD is a report from a consignee that he did not receive a shipment, or that there was a difference between the cargo as described on the TCMD and that actually received. Either case will probably require a military police investigation, using the TCMD as a starting point.

d. Two physical aspects of the cargo checking activity may be worthy of consideration:

(1) When the cargo vehicle gates are also used by other traffic, a turnout may be provided into which cargo vehicles can be directed for checking. This turnout, of a size appropriate to the volume of traffic, will eliminate congestion at the gate.

(2) To facilitate checking of cargo, a wooden platform may be built at the checking area. The platform should be as long as the vehicles being used (e.g., tractor-trailer) and provide a deck at, or slightly higher than, the level of the truck bed. Such a platform provides for easier and quicker checking since it permits better observation of the cargo.

e. Military police assigned to terminal cargo checking duties should be thoroughly familiar with the procedures for use of the TCMD and allied documents (see appendix T).

10-8 Container Operations

Cargoes intransit are vulnerable to overt hazards (such as pilferage, and enemy or guerrilla attack or ambush) and covert

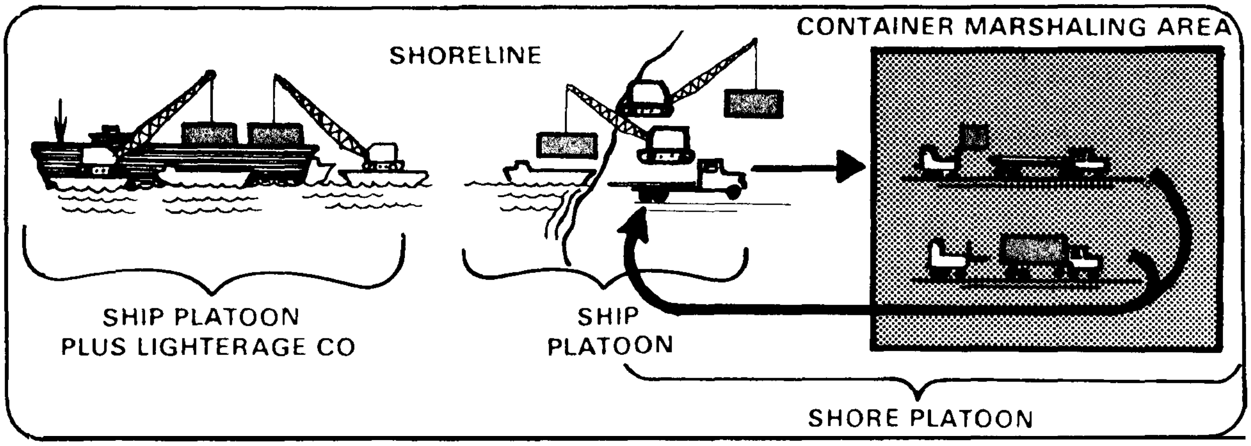


Figure 71—Vulnerable stages for theft / pilferage of cargo.

hazards (such as sabotage). As one measure to provide additional security for supplies and equipment, the use of containers during shipment is widely used.

a. Containers must receive close security emphasis during:

■ Filling
■ Sealing
■ Storage (shipper/receiver)
■ Shipment (onloading and offloading),

b. Areas where security measures for containers must be stringent are (figure 71):

● On board ship
● Shoreline transitions
● Container marshaling area.

c. Knowledge is the keynote to security during container operations. It is important that security personnel be aware of the following to detect pilferage and theft:

■ Packaging, labeling and placarding requirements.
■ Cargo compatibility characteristics and segregation requirements.
■ Container and cargo handling and safety measures.
■ Actions to be initiated in case of suspected pilferage/theft operations.
■ Speical storage, identification and movement requirements.
■ Pertinent regulations and publications.

d. Some basic measures for beefing up security are discussed next:

(1) Marshaling yard entrance/exit. Control of vehicular and pedestrian traffic entering and leaving the area is a must:

■ Establish a single control point for each.
■ Man both points with US military personnel assisted, as required, by foreign national police and/or interpreters.

(2) At the vehicular control point:

❑ Prevent entry of unauthorized vehicles (only transporter and materials handling equipment, maintenance, and essential administrative vehicles may enter).
❑ Inspect inbound and outbound containers for:
• Evidence of damage or unserviceability.
• Presence and condition of container seal and/or lock.
• Evidence of illegal entry into container (such as tampering with or removal of door hinges).
• Stolen items, particularly with outbound containers (look on top and under container, and inspect transporter cab).

❑ Verify documentation for correctness, completeness, and legibility (check that the transporter number, container number, and container seal number match those shown on the TCMD).

❑ **No container (inbound or outbound)**

passes through the control point without a valid TCMD.

(3) At the pedestrian control point:

- Permit only authorized personnel to enter container marshaling area.
- Establish, maintain, control, and safeguard a pass system for persons authorized to be in the area:

- A photo-bearing, serially numbered, plastic-enclosed pass can be prepared for each individual authorized to be in the yard. The individual picks up the pass when entering through the gate and returns it to the security guard upon leaving.
- Further refinement of the pass system may be made by color-coding to indicate the specific area of the yard in which the bearer is authorized. Color-coding can be made even more visible by requiring hard hats that reflect the same color as the pass.

e. A physical security officer (military police) is authorized in the security, plans, and operations section of the transportation terminal battalion. He is responsible to the battalion S3 for developing, putting into effect, and monitoring the marshaling area security plans, procedures, and actions. His responsibilities also include determination and supervision of the force (for example, military police units) required for terminal security.

f. Perimeter security of the marshaling yard backs up gate security in keeping unauthorized people out of the area. Unauthorized people may engage in sabotage (particularly in an ammunition marshaling area) or petty theft. Or, to promote large-scale theft operations, they may establish inside contacts with people working in the yard. Perimeter security measures may include one or more of the following:

(1) Chain type fencing topped by strands of barbed wire. Inspect fence daily to assure there are no holes or breaks (chapter 5).

(2) Concertina wire (chapter 5).

(3) Flood lighting (chapter 6).

(4) When feasible, use of sensors and IDS systems (chapter 7).

(5) In a LOTS operation, mine strips on the land side.

(6) Use of motor patrols, dog patrols, and physical security posts, which, upon request, can be made available by the military police physical security company (TOE 19-97).

g. Security cargo. Though it may not be possible to fence the entire yard, the security cargo (that is, sensitive, classified, and high-dollar-value cargo) area should, as a minimum, be fenced with its own military guarded gate and MP patrol. An added security measure is the **stacking** of containers **door-to-door,** or with the door against a wall (also applicable to other types of cargo). (See figure 72 for example.) The break-bulk point and damaged cargo storage area are

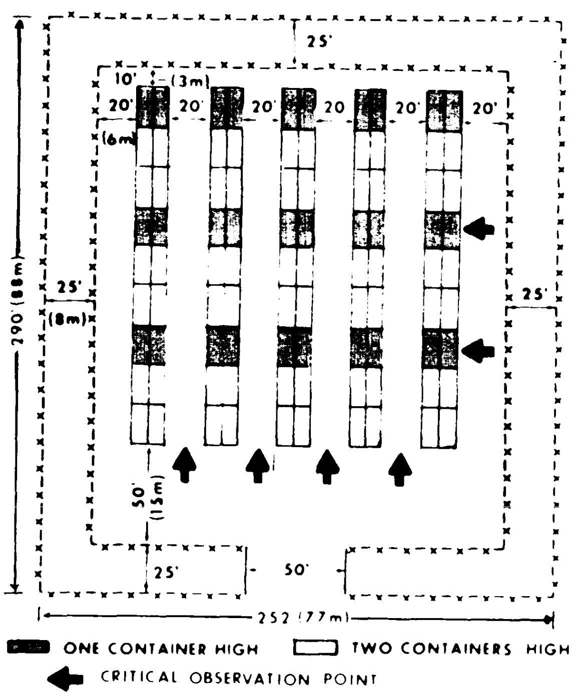


Figure 72—Details of stacked containers for maximum security

also potential high loss areas and require close supervision and/or adequate perimeter barriers and lighting. Additionally, whenever possible, security cargo should be unloaded from the ship during daylight hours. Observation of unloading operations by MP security personnel is highly desirable.

h. Safeguarding and controlling TCMDs. Normally TCMDs are not accountable documents. If desired, TCMDs may be serially numbered locally to aid in control and to discourage pilferage of the form for illegal use. Regardless of other measures, blank TCMDs should be secured, with one individual responsible for their safeguarding and issue. Completed TCMDs should be kept in a vault file to prevent unauthorized alterations or destruction to remove evidence of cargo diversions/pilferage.

i. Safeguarding and controlling container seals. A container seal is a device applied to the container door fastening to indicate whether the door has been opened or the fastening tampered with and, if so, at what point in the movement system it happened. Seals are serially numbered to help indentify the person who applied the seal and to provide control. Unless seals are strictly accounted for from receipt to application, their purpose (to pinpoint unauthorized entry into the container) is defeated. Container seal control and accountability is promoted by the following procedures:

■ Maintain a record by serial number of seals—

❑ Received by the port operations officer.
❑ Issued to authorized persons for application to containers.

■ Store seals under lock.
■ Designate one person to be responsible for safekeeping, issue, and recordkeeping of seals applied at the port.
■ Designate specific persons on each shift to apply seals (keep number of persons to a minimum).
■ Enter serial number of seal on TCMD.
■ Conduct periodic inventory of seals.
■ Seals should be applied—

- As soon as container has been stuffed.
- As soon as a stuffed but unsealed or improperly sealed container is detected.

■ An inventory of contents may be required if sufficient evidence exists that cargo has been pilfered. In an y case appropriate entries must be made on the TCMD to indentify any change in seals.
■ Application of seals should be supervised. Failure to supervise, or allowing a yard hostler to move an unsealed container to the stacking area, offers opportunity to—

- Pilfer cargo prior to applying the seal.
- Apply a bogus seal, break the seal later, remove cargo, and then apply the legitimate seal.

10-9 Anchorage Security

When a port lacks sufficient pier space to accommodate traffic, ships may be required to anchor, or even to load and unload, offshore. Positions of ships in anchorage are assigned by local port authorities. Cargo is loaded or unloaded by lighters (large barges) which also transport stevedores to the ship being worked. This type of operation has advantages and disadvantages with respect to security of the ships. The trips to and from anchored ships give added time for inspection or surveillance of the laborers; but it is difficult to control movements of small boats that bring provisions to the ships. Such craft may be used in pilfering, smuggling, or sabotage activities. Military police water patrols and alert supervision of stevedoring offer the most effective protection.

a. Shipboard Guards.

(1) In addition to hatch guards, guards must be assigned, where appropriate, to the decks of ships at anchor.

(2) Deck guards may be assigned to either stationary or walking patrols. In addition to cooperating with hatch guards, the

following duties may be included:

(a) Security of' cargo stowed on deck.
(b) Security of cargo being unloaded onto lighters.
(c) Observation of small craft in the vicinity of the ships at anchor.
(d) Observation of surrounding waters to detect any attempted approach by swimmer sappers.
(e) Assistance in operating the anchor chain collars.

(3) Deck guards must be able to communicate, preferably by radio, with harbor patrol boats either directly or through their operations center.

(4) Deck guards must have appropriate foul weather clothing; binoculars are essential for proper observation of surrounding waters and small craft.

b. Anchor Chain Collar.

(1) Swimmer sappers use the anchor chains of ships to their advantage. They tie one end of a line to them and on the other end attach their mines. When the current changes, the mine moves alongside the ship and explodes. To prevent sappers from accomplishing this goal through this technique, anchor chains must be checked frequently. This can be done from aboard ship.

(2) A simple device has been discovered to help personnel aboard ship check the anchor chain. This device is the anchor chain collar (figure 73). It is built with two padeyes—one at the top of the collar and one at the bottom. The padeye at the top is used to connect the rope used to haul the collar up, dragging any attached sapper

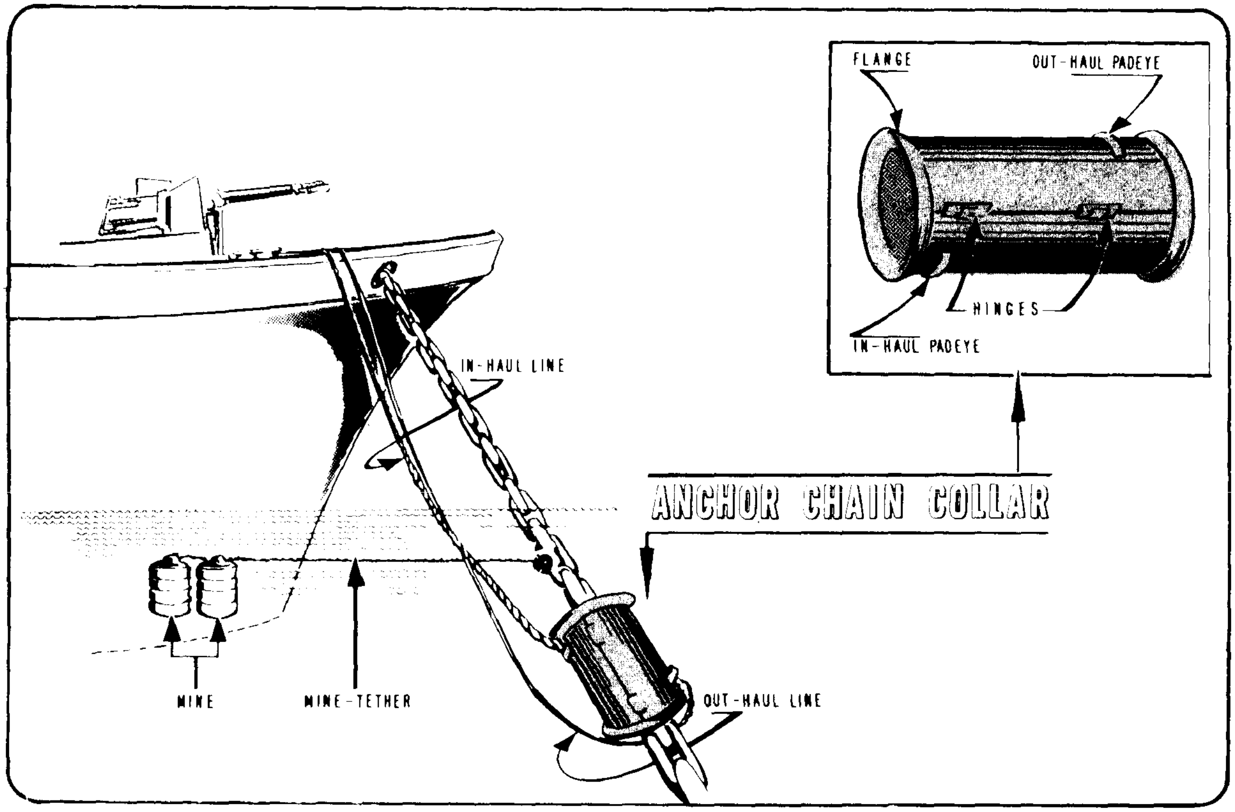


Figure 73—Anchor chain collar details.

line out of the water. The lower padeye is used to connect an out-haul line which is threaded through the link in the anchor chain at the anchor ring. The collar can thus be raised by hauling the collar up, and lowered by pulling in the out-haul line. Raising and lowering the collar should be done every 15 to 20 minutes on an irregular basis. A detail of the collar (ring) is depicted at figure 74.

(3) No specific dimensions are set for the collar since one standard collar will not fit all sizes of anchor chains. Collars should be fabricated (by engineer, ordnance, or naval units) in sizes appropriate to the sizes of anchor chains most commonly in use in each area—preferably the largest size since it can be used also on smaller sizes. The collar should be, generally, twice the length of the anchor chain link; the width should be sufficient to leave 3 to 4 inches of free space on each side of the link, to allow for accumulations of seaweed or debris.

(4) A port commander should have one of these collar devices available for each ship that anchors in his area of responsibility. Collars could be issued to each vessel as it arrives and returned to port authorities just prior to the ship's departure. Ships' captains should also be encouraged to fabricate their own collars for use while in hostile waters, thus insuring they will

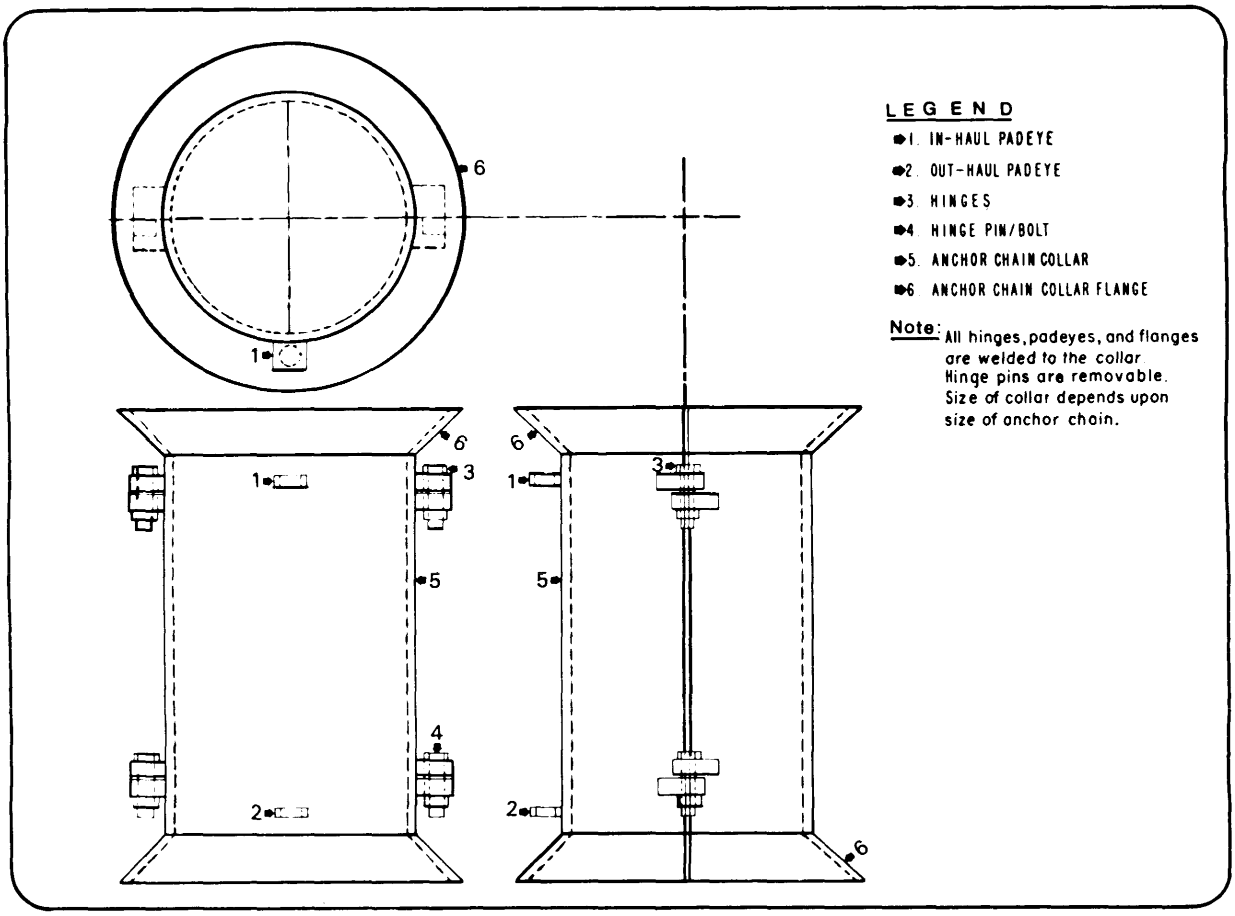


Figure 74—Details of anchor chain collar design.

always have a collar available while they are at anchor.

(5) Personnel operating and checking these collars must be instructed that:

(a) Lines must be kept taut while the collar is in place. Any slack observed in the line must be considered as possible tampering with the line (cut by an underwater swimmer) and must be promptly investigated.
(b) If the line cannot be hauled in, an investigation must be made to determine the reason. It may have been cut by an underwater swimmer and tied to the anchor chain to prevent hauling in the collar.

(6) When mines are suspected or discovered, EOD personnel should be contacted immediately through the port commander so that mines can be detached and made harmless.

10-10 River and Harbor Patrols

a. Port and harbor security requires the use of patrol boats, not only for the open harbor area but for the water sides of piers, dock areas, and patrol of inland waterways and beach areas used in LOTS operations.

b. Missions assigned to military police water patrols may include the following:

(1) In port areas:

(a) Enforce port regulations.
(b) Suppress criminal activity.
(c) Provide offshore security for quays, piers, moorages, and anchorages.
(d) Provide offshore security for communication facilities, port security devices, and aids to navigation.
(e) Provide security for incoming and outgoing craft, moored or anchored craft, and lighter operations.
(f) Assist in circulation and control of individuals.

(2) In beach or river shore areas.

(a) Any of the missions in paragraph (1) above.
(b) Support beach or shore parties in regulation, control, and direction of watercraft near the beach or shore.
(c) Guide troop or cargo carrying small craft between larger craft and beach or shore points.
(d) Guide, escort, and guard small craft engaged in high priority movements of wounded personnel, emergency supplies, command and staff groups and designated persons.
(e) Guard craft transporting, loading, or unloading prisoners of war, and guard offshore areas at prisoner-of-war assembly points.

(3) At military installations. Patrol activity on waterways that form the boundaries of or pass through a military installation may include any of the missions in paragraphs (1) and (2) above applicable to the installation, and:

(a) Guard waterways to prevent their use for unauthorized entry or exit.
(b) Provide security for facilities and equipment, power and communications line, etc., located on or adjacent to waterways.
(c) Enforce hunting, fishing, swimming, boating, camping, fire prevention, and forestry conservation regulations on and adjacent to waterways.
(d) Enforce off limits regulations pertaining to firing ranges, impact areas, demolition areas, restricted areas, and similar areas on or adjacent to waterways.

c. The MP company assigned the mission of river and harbor patroling is the “Military Police Company River/Harbor Security,” TOE 19-287. Review this TOE for personnel strength and unit operational capabilities and limitations.

d. Water Patrol Operations. River and harbor security operations require continu-

ous coordination and liaison with land-based MP organizations and with indigenous military or civil police operating in the same area of responsibility.

(1) Extent and nature of coordination necessary for effective use of this support varies with the activity supported. But the company commander and his physical security officer must also maintain close operational liaison with the headquarters staff element responsible for such physical security planning in order to implement operating instructions.

(2) Waterborne patrols provide the only practical means available to effectively protect arterial and smaller waterways and pier facilities (to include such sensitive installations as tank farms and pumping stations) against waterborne threat. In carrying out their security activities, personnel of this functional support unit assist the terminal commander in the discharge of his responsibility for the security of military cargo in terminal facilities and support the area commander in security of in transit supplies through his area of responsibility.

(3) Two additional platoons and supporting maintenance elements may be attached to this organization, depending on range of waterway areas to be covered. Conversely, platoons and their organic patrol craft sections may be detached where required for support of separate facilities.

(4) Water patrol operations should be conducted as an extension of and a supplement to shore-based MP operations. Operational procedures and techniques prescribed in military police training publications (FM 19-series) should be followed.

(5) Water patrol activity includes all the dangers normally encountered by military police plus the possibility of encounters with dangerous waterfront criminals or enemy/insurgent forces and of accidents on the water. A thorough and continuous consideration of safety, communications, support, and reserve factors is a must in water patrol operations.

e. Planning. Water patrol routes and missions are assigned in accordance with the need for MP service. The need is determined by:

(1) A survey of actual and probable criminal or enemy activity that can be suppressed or prevented by water patrols.

(2) An estimate of the number, type, and location of water patrols required.

f. Prevention of waterfront criminal or enemy activity is based upon adequate physical security measures to provide protection for Government supplies and equipment. Physical security measures may be supplemented by water patrols that perform the following:

(1) Observe activities of watercraft and persons aboard watercraft.

(2) Observe activities of persons on the waterfront and shoreline.

(3) Suppress trafficking in controlled and pilfered items between the shore and watercraft, and between watercraft.

(4) Investigate and report any suspicious actions on the part of persons or watercraft.

(5) Enforce off limits regulations pertaining to, and provide offshore security for, communications facilities, port security devices, aids to navigation, dock facilities, moorages, and anchorages.

Chapter 11

Computer Security



Expensive equipment and sensitive information is usually concentrated in a military computer complex. The importance of the Army computer complex has increased correspondingly with the use of automatic data processing (ADP) in a variety of military activities. Protective security measures should be established for the equipment, information, operational programs maintained in the complex, and for the facility that houses the processing, main storage units, and remote components.

Computer complexes are susceptible to the security hazards discussed in appendixes B and C. Additionally, magnetism poses a possible threat to the computer complex. A magnet, depending upon its size and location, can scramble recorded data. Also, strong radar signals can interfere with the operation of data processing equipment.

An integrated staff effort is recommended for formulating and executing a security program for a military computer complex. The user is responsible for classification of informational elements contained in the input, data base, and output. At the local data processing installation (DPI) level, the systems security officer has staff responsibility for security of the facility in which the machines are located, to include remote terminals. Local military intelligence has staff responsibility for security of the data contained within the machines.

The physical security expertise available in the provost marshal's office should be used to the maximum extent, and should be complemented by the technical knowledge in other staff areas, such as management information systems, communications and electronics, security office (G2/S2), facilities engineer, fire and safety. Computer expertise, not organic to the installation, may also be considered as a source for additional information and advice.

11-1 Physical Protection

Primary considerations should be the building design and the corresponding applicability of protective measures.

a. Building Design. This includes both existing structures and those being planned and under construction. Selection of protective measures may be influenced by the construction materials used to meet building specifications. Existing physical security measures should be reevaluated as part of the planning process for future modification, expansion, or renovation. Considerations in the selection of a location for the computer complex should include whether it will be:

(1) Housed in one or multiple buildings.

(2) Positioned on one or more floors of the buildings.

(3) Other activities located around it.

(4) Exposed to hazards described in appendixes B and C.

> **Note:** Ideally, a DPI should be located in a separate building. This increases the feasibility of applying appropriate physical protection. Alternatively, it should be located on the second floor of a multi-story structure. This reduces unnecessary pedestrian traffic around the DPI and thus reduces the possibility of unauthorized persons gaining access to or observation of DPI operations.

b. Protective Measures. Computer complexes may require differing degrees and types of protection depending on the physical characteristics of each location, surrounding environment, and vulnerability to security hazards (see figure 75).

(1) Physical security measures may include:

(a) Protective barriers consisting of fences, gates, and doors (chapter 5).
(b) Locking systems (chapter 8).
(c) Protective lighting (chapter 6).
(d) Security force personnel (chapter 9). In some cases well trained receptionists can perform the same duties as security personnel during normal working hours.
(e) Personnel movement control (chapter 4).
(f) Intrusion detection systems (chapter 7).

(2) Electric power. Without electrical power a computer complex cannot operate.

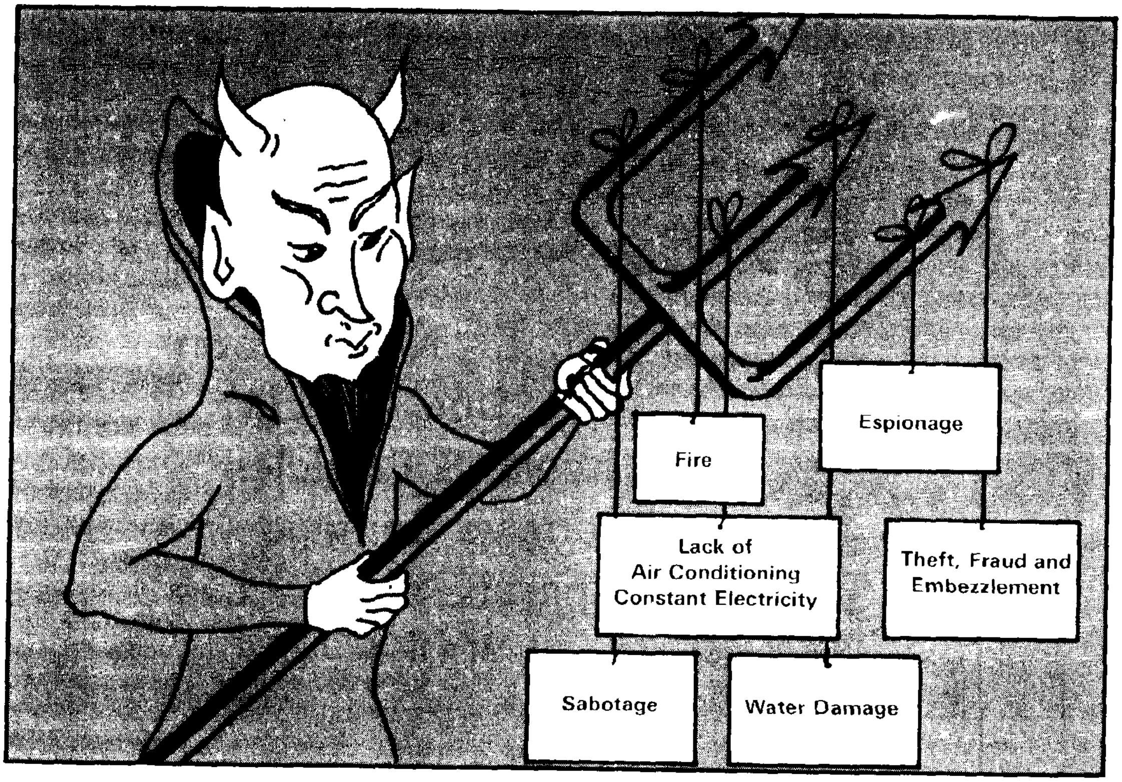


Figure 75—Computer hazards.

All power sources to the computer complex must be continually protected. Three specific problems dealing with electrical power are:

(a) Transients are temporary oscillations that occur in a circuit due to a sudden change in voltage or load. This sudden change can cause errors in passage of data within the computer.
(b) A brownout is a short period of curtailment in electrical power; however, it lasts longer than a transient.
(c) A blackout is the same as a brownout but for an extended period.

(3) Emergency power. This energy source should be available to insure continuous operation of the computer complex. There are at least two types of emergency power available—dual feeds and genera tor.

(a) Certain military installations may maintain their own power source and also use commercial power. Dual feed would incorporate both on post and commercial power sources into the computer complex. There should be emergency cutoff switches for all electrical utilities at every exit from the DPI. Such switches will break every electrical circuit when thrown and will minimize damage from electrical fires.
(b) There are many different generators that can provide an alternate power source to the computer complex. Costs of alternate power sources are high but may be necessary to insure continuous operation of the computer complex.
(c) Loss of power may be caused by natural or manmade reasons. Physical security planning should include measures to prevent or minimize the effects of power losses.

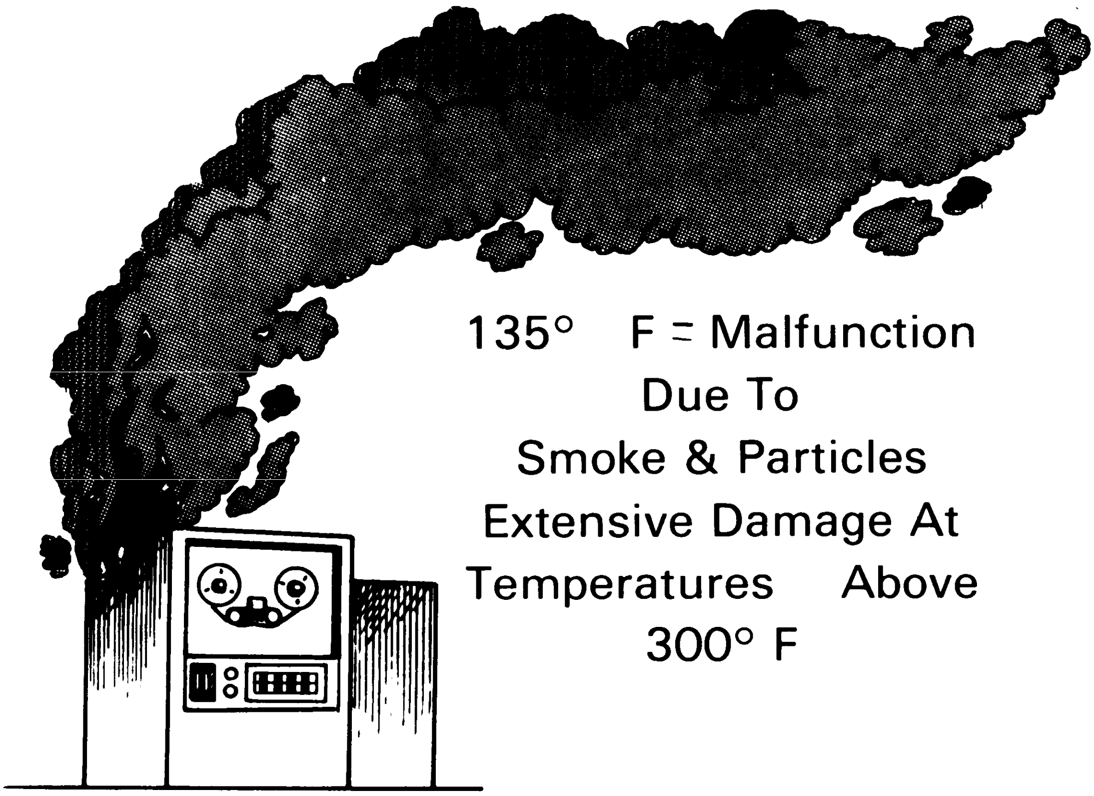


Figure 76—Fire dangers for computer equipment.

(4) Fire prevention. To insure against destruction of the computer complex by fire, comprehensive fire prevention measures should be undertaken (figure 76). Considerations should include the type of construction of the building that houses the computer complex, location and general cleanliness of the area, and the degree of housekeeping within the computer center (ARs 18-1 and 18-2).

(a) Alarms and detectors. The locations, sizes, and functions of alarms and detectors are important in considering fire prevention.

(b) Fire extinguishers. There are a variety of fire extinguishing agents available for use in a computer complex. These extinguishers must be chosen carefully to insure they do the least damage to computers and still extinguish a fire.

(c) Firefighting teams. Any fire control plan must insure that qualified, trained, and efficient personnel can properly use existing fire control devices. They should be-trained to fight a fire in the computer room with minimal damage to computer equipment.

(d) Protective covering. The use of equipment protective coverings can reduce fire and water damage in case of a fire.

(e) Emergency utility procedures. Water and electrical utility cutoff procedures should be specified in case of fire or other disaster.

(5) Air conditioning is required for most computer complexes. A computer complex should have its own air conditioning system. It should not be dependent upon the system that is used for the entire building. The fresh air intakes should be so located as to prevent smoke, dirt, or dust from entering the computer complex. They should contain filters. Periodically the intakes should be inspected to insure

proper operation. Air conditioning systems for a computer complex should have performance monitors. The placement of these monitors is important. Improper placement may cause the system to operate incorrectly. Emergency power sources must also be capable of handling air conditioning systems within the computer room because most computers cannot operate without air conditioning.

(6) Housekeeping. The enforcement of good housekeeping practices increases overall security for computer operations (AR 18-2).

(a) Smoking and eating in the computer room should not be allowed. A cup of coffee accidentally or purposefully spilled on a computer mainframe or tape drive unit could cause extensive damage.
(b) Trash containers within the computer room should be made of fireproof material and have properly fitting lids.
(c) Fire extinguishers should be stored so they are readily available when needed.
(d) Proper disposal of input and output media is important. In the hands of unauthorized persons, this information could be compromised and could lead to breaches of national security.

(7) Water damage. The following two areas of concern are important in preventing water damage to the computer room:

(a) Natural flooding. Surface water within the computer room is possible if the room is located on the ground floor or basement of an area subject to flooding. Storms may cause damage to the computer room if it is located on the outer wall of a building containing large glass windows.
(b) Manmade fixtures. Plumbing should not be allowed to run over, under, nor alongside the computer room be cause extensive damage could occur if such pipes should burst. Floor drains, sump pumps, and protective equipment coverings may minimize water damage to the computer room.

11-2 System Integrity

a. Hardware is the physical equipment or devices forming a computer and its peripheral equipment.

(1) Alternate data storage refers to equipment/files available as auxiliary or backup to the primary computer system. Alternate storage should not be located in the same computer room with the primary system. Physical security of the alternate should be similar to that of the primary system.

(2) Computer maintenance on hardware is a continuing process. It may involve an unscheduled stoppage or normal preventive maintenance. Knowledge and supervision of maintenance personnel are important. Security requirements differ depending upon whether maintenance is performed by internal or external services. Physical security standards must be strictly enforced during maintenance operations.

(3) Key punch equipment and locations should have physical security equivalent to the material being prepared or punched.

(4) Computer terminals require physical security procedures based on their performance requirements. Location of the system user must always be considered when setting up a system with various station locations. A given user may have full authoritative access to certain information, but certain locations may not have access to that information because of unauthorized persons in the area. Security technical protective measures should be directed toward these areas:

(a) Data controls
(b) Access controls
(c) Password controls.

153-846 O - 94 - 10

(5) Secure handling of sensitive and classified information should be emphasized to everyone in the computer complex.

b. Software refers to the program and routines used to extend the capabilities of the computer.

(1) Necessary security precautions should be implemented to insure knowledge of who writes the program, where they are written, where they are tested and filed and what is the security classification of the program.

(2) Data file systems contain information that can be processed or produced by the computer. These files must be provided a degree of security commensurate with the importance of the files. A typical data file system allows for the creation of a unique file with the establishment of a password when the file is created. The system must respond to the privacy of the password itself, and must prevent printouts or readouts or system reviews that would reveal the password. In addition to passwords, some files are further protected by a *permissive* system. The names of valid users should be explicitly stated as having certain very specific access to the file, such as *read* or *write.* In this manner a file can be put to its maximum use by allowing differing and restricted use simultaneously to various users at various levels of authority.

(3) Documentation provides the historical reference record of data file systems and programs. The same degree of physical security should apply to documentation as in paragraphs 11-2a(2) and (3).

c. For further guidance in this area, see AR 18-2.

11-3 Procedures and Control

Procedures and controls encompass the entire area of operation concerning the computer complex. The areas of interest are diverse, as the following example shows:

a. Separation of Duties. In most computer complexes, personnel are divided into several functional groupings—programers, operators, librarians, data preparers, and data controllers. These are in addition to internal audit personnel and the security force, which are usually independent of data processing operations. It is not always necessary or possible for these groupings to be separate and distinct; but in a large computer operation they should be so grouped. The **security classification of** these personnel must be **commensurate with the level of classification of the data or program that they are processing or developing.** This factor is highly significant in the staffing and use of personnel.

b. Rotation of duties is sound personnel management and an essential control.

c. Production schedules should contain run authorizations, time estimates, data file and program library release memoranda, data preparation instructions, output routing and input and output checking guides. All production work should be run according to the schedule and all program development should be controlled separately.

11-4 Protection Of Crime Scenes

a. A breach of physical security is, in most instances, a crime; and the scene of the breach must be treated as such. The first principle is to **refrain from disturbing it.**

b. Protection may then be afforded to the scene through the use of other security forces on fixed posts, roving foot patrols, motorized patrols, or by roping or blocking off the area with available materials such as ropes, boxes, or boards (see TC 19-23).

c. Complete protection is essential to **insure that no evidence is moved** until the investigators can record its exact location and condition by the use of notes, sketches, photographs, or other means. Protection also preserves the integrity of the evidence for proper identification and evaluation, and enables investigators to correlate the evidence with the crime and crime scene.

11-5 Personnel at the Scene

a. Persons at or near the crime scene must be considered as part of the scene and must be identified. Where appropriate, and where jurisdiction of place and persons is clear, they should be detained at the scene and released to investigators.

b. Any questioning of such personnel must meet the requirements for warning of rights under the Manual for Courts Martial, and the Fifth Amendment to the Constitution must be strictly observed, since they may later be considered as suspects, and any improper questioning could prejudice any disciplinary or legal action against them. Careful and complete notes should be made of any spontaneous or voluntary information they offer, or any remarks they make.

11-6 Assistance To Investigators

Security force personnel can assist investigators in numerous ways, both at the scene and during later phases of the investigation. Protection and control of the scene is, of course, the first consideration. Nothing should be disturbed or removed until it is released by the investigators.

a. All information obtained should be turned over to investigators immediately upon their arrival.

b. Provide investigators with any information they request relative to the installation, scene of the breach of security, activities and personnel pertinent to the situation. Such information may include observations as to vulnerability of the area, which permitted the breach of security to occur reports of previous incidents of the same or similar type, when and where they occurred, and their effect on routine operations of the installation; and information concerning the security classification of the area, if any, and the pass or badge system or other personnel circulation control measures (chapter 4).

c. Security force personnel can also provide facilities for the questioning of persons; can insure that personnel are available for questioning; and if apprehension is necessary, provide information as to where the subject can be located and what assistance can be rendered by the command to facilitate apprehension.

d. The security force may also assist investigators, at their request and under their direction, in searching for, locating, and preserving any physical evidence pertaining to the breach of security. In such activities, caution must be exercised to avoid any action that would contaminate or impair the integrit y of the evidence. Evidence must be handled—if at all—strictly in accordance with the directions of investigators, who are ultimately responsible for it.

e. Security force personnel should be familiar with the provisions of FMs 19-10 and 19-20 with respect to handling and preservation of evidence, and adhere strictly to those provisions.

f. Run Control Log. This log should contain detailed records of all runs, errors, interruptions, and restarts. For sensitive operations, a console printer, recording all of the operations listed above, may be located remotely or in a secured part of the computer complex.

g. Operations Review. Sound management of a computer complex requires that actual performance be compared to scheduled

performance and any variations be noted, investigated, and explained. Production schedules and run control logs are essential inputs to this process.

h. Input and Output Control. Quality control and checks of all input and output should be maintained by a separate data control group. Special efforts should be made to insure that data accepted by data control is not altered prior to processing. This is required not just for control, but is essential for detecting and correcting errors.

i. Program Change Control. Changes to production programs should occur only upon authorization. Verification of any change should be made by the internal audit group prior to replacing the audit copy in the library.

j. Master File Control. Master file changes should also be made only by authorization, and should be subject to an internal system of checks and balances.

k. Rigid Control of Passwords. In a teleprocessing environment, passwords should not be assignable from the console, nor transmitted to users by telephone. Wherever possible, terminal identification and password match should be required.

l. Auditing Support. Skilled and experienced audit personnel on the installation may increase computer security by participating in the development and maintenance of standards and procedures for systems design, programing, and operations.

m. File Protection Devices. Maximum use of file protection devices and techniques will assist in preventing accidental or willful destruction of data files.

n. Manual Operations. Systems design should include provisions for short-term manual operation whenever possible in the event normal operations are disrupted.

o. Hardware Monitoring Prevention. An independent survey by technically qualified persons should be conducted at all computer facilities to determine external hardware emissions and methods available to reduce or eliminate emissions capable of being recorded by undesirable sources.

11-7 Evacuation And Contingency Planning

a. Evacuation planning should be initiated to insure that immediate and effective action is taken in case of required evacuation of the computer complex due to fire, flood, bomb threat or enemy action. These plans should include:

(1) Procedures for securing and priority evacuation of certain data files.

(2) Criteria for destruction of hardware, software, and data files prior to evacuation.

b. Contingency or emergency planning is important in case the everyday operation of the computer complex is disrupted or completely destroyed. Contingency planning should afford the ability to continue operations using auxiliary power sources and alternate equipment.

c. Further guidance in this area is found in AR 18-2.

11-8 Computer Security Program

Computer security is the sum of man y parts. A total security program should include a blend of procedural safeguards, an interface of physical protection, personnel selection, and audit controls. There should be an integration of all interdependent features.

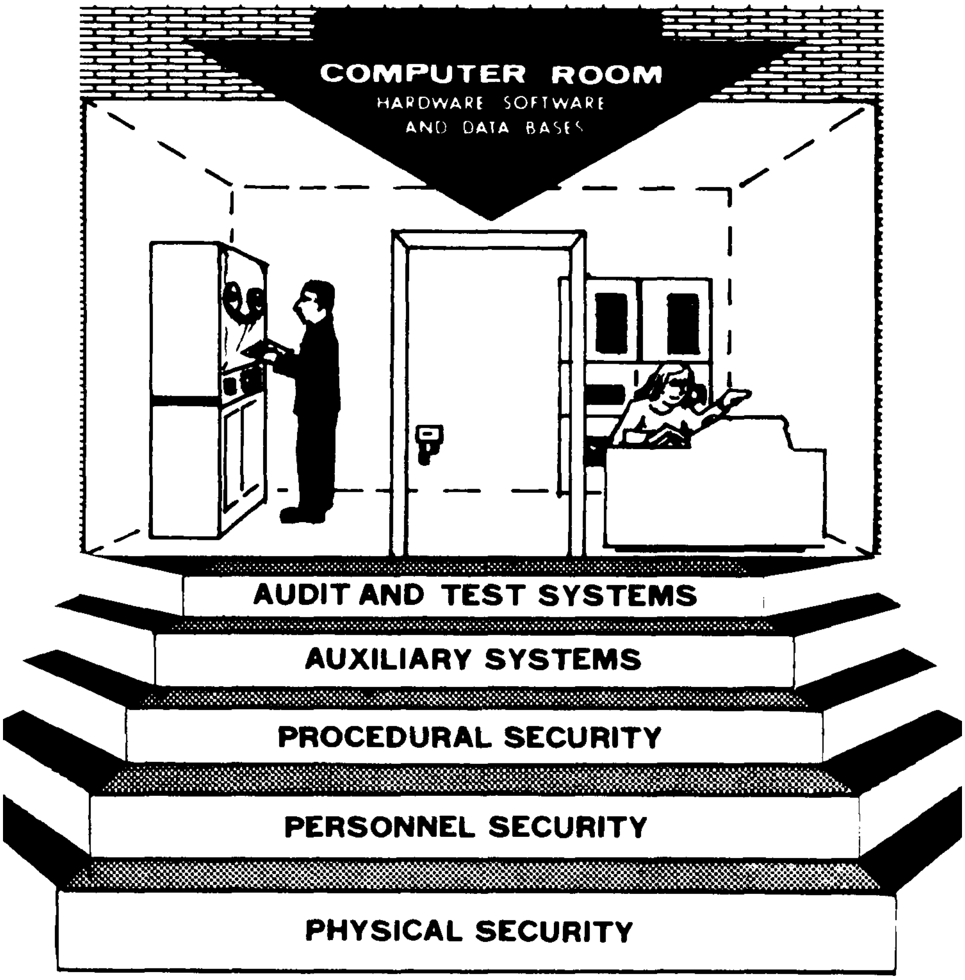
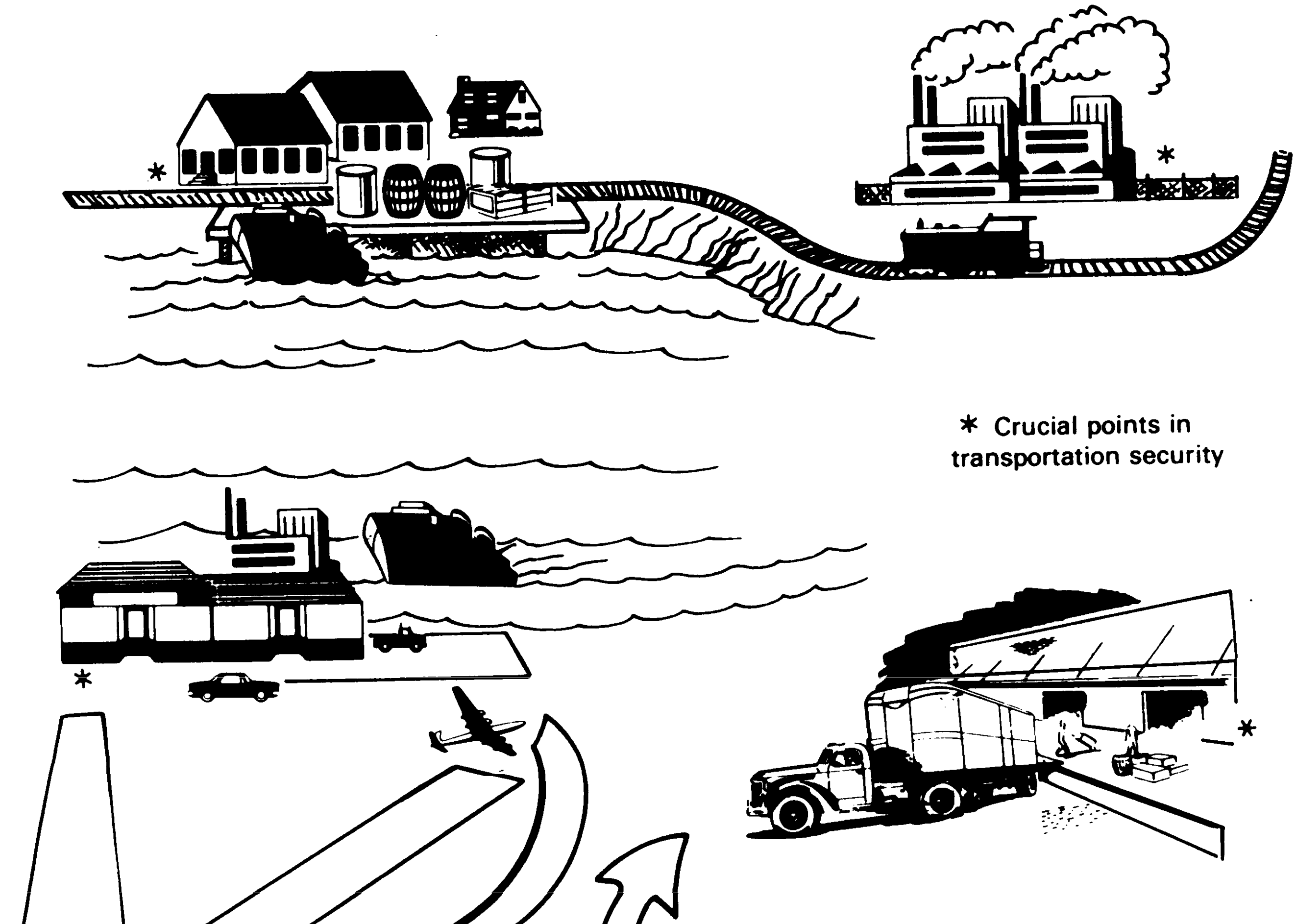


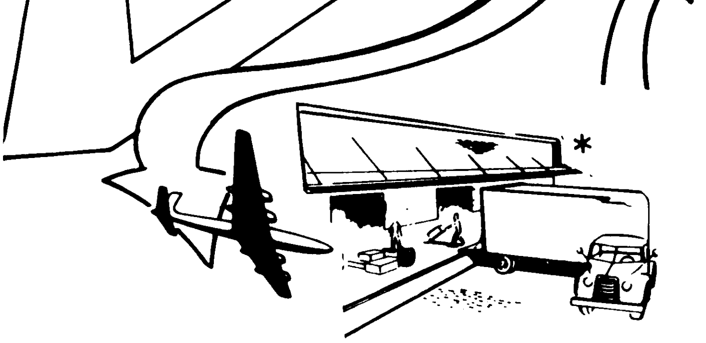
Figure 77—Five steps to computer security.

Where possible, each of these individual controls should be built into the computer system at the start. An effective program is a continuing one.

Chapter 12

Transportation Security





Transportation security has evolved to encompass all security measures taken to protect shipments from criminal/terrorist activity. The types of shipments include:

- Classified
- Hazards
- General cargo
- Combination of these
- Protected
  - Pilferable
  - Sensitive
  - Controlled

There are no universal or one-time solutions to the problems of cargo security, because each mode of transportation and type of shipment in each shipping/receiving terminal, and each transfer point is unique. However, certain basic principles of cargo security can be adapted to accommodate any mode of transportation or any facility—large or small.

12-1 Considerations

a. The following general considerations should be adhered to when shipping cargo:

(1) Exercise management obligation directly or through a security manager responsible for the shipment (appendix I).

(2) The threat, sensitivity of cargo, vulnerability, and mode of transportation dictate the degree of security required during storage and in transit (chapter 1).

b. The degree or type of security needed is determined by:

- Facility size and location.
- Complexity of storage or shipment.
- Volume/value of items.
- Economic and geographical situation.
- Available crime statistics.
- Security/law enforcement available.
- Transit shipments.

These factors may change as the cargo is moved from one area to another.

c. Development of an effective cargo security system should be based on:

- ☐ Experiences of personnel responsible for shipments and storage of cargo.
- ☐ Loss potential based on a risk analysis as outlined in chapter 2.
- ☐ Established security standards and policy.

12-2 Physical Security Cargo Plan

To insure that adequate security is assessed, it is imperative that a security cargo plan be developed to cover all forseeable contingencies and be flexible to meet ship ment/storage needs.

12-3 Pilferage

The following characteristics apply to pilferage in the transportation environment:

a. Difficult to detect because pilferers usually operate alone.

b. Evidence is hard to obtain because of the complexity in the shipment and storage system.

c. A primary concern of the security program involving transportation and storage of items.

d. Unsystematic in nature.

e. Commonly occurs in a terminal while cargo is awaiting movement from one vehicle or mode of transportation to another (figure 78).

f. Most often committed by employees of the carrier service.

12-4 Pilferage Prevention

To prevent transportation pilferage, apply these steps:

a. Analyze existing conditions (chapter 1).

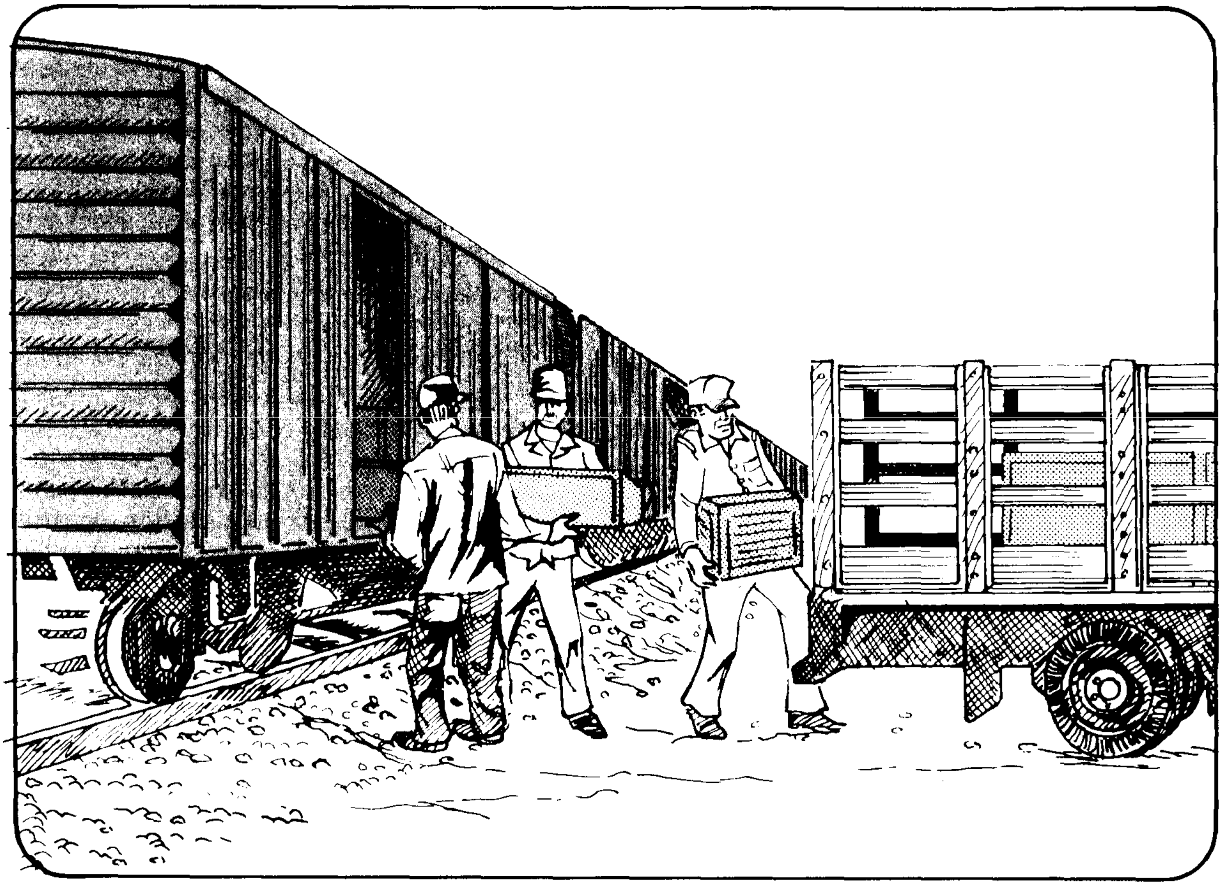


Figure 78—Transshipment areas are most vulnerable to pilferage.

b. Control presonnel movement (chapter 4).

c. Use a parcel check system (chapter 4).

d. Exclude privately owned vehicles from parcel checkpoint (s).

e. Stress the moral wrong of pilferage (chapter 3).

f. Apply stringent accountability procedures (chapter 4).

g. Insure high employee morale (chapter 3).

h. Develop respect between security personnel and employees.

i. Incorporate active security measures in a security in depth configuration.

12-5 Theft During Shipment/Storage

a. Theft prevention is management's first responsibility (see appendix I).

b. A systematic and planned theft or other

crime is frequently committed with accomplices and usually involves:

- An available market.
- Goods that are profitable and easily disposed of.

12-6 Areas And Functions Vulnerable To Manipulation

The following are considered areas and functions with high theft potential:

- Terminal operation areas
- Truck drivers
- Facility personnel
- False invoice shipments and receipts.

12-7 Management Controls

To minimize exposure to individuals who display a motive to steal, the security manager should:

a. Illustrate and use countermeasures.

b. Screen prospective personnel.

c. Eliminate in-facility gambling among employees.

d. Eliminate the get-even attitude among employees.

e. Reduce exposure of cargo to theft and pilferage.

f. Insure close coordination between packaging, shipping, and receiving personnel.

g. Increase the probability of detection when thefts do occur.

h. Discipline those persons apprehended for theft and pilferage.

i. Obtain feedback to determine whether promulgated cargo theft countermeasures have, in fact, been implemented and are being properly followed by operating personnel.

12-8 Special Security Considerations

Because the following items are part of military life and easy to pilfer, and because there is a demand for them on the black market, special security considerations are necessary:

- Weapons
- Ammunition
- Electronic items
- Photographic equipment
- Class VI items.

(See appendix U, p. 494 for classes of supply.)

12-9 Shipper Awareness

Shippers, to reduce theft of cargo, should be familiar with:

- ☐ Packing requirements and procedures.
- ☐ Receipt procedures at destinations.
- ☐ Provide advance notice of shipments to receiver.
- ☐ Arrival and departure times of all cargo shipments.
- ☐ Specific routes of travel.

12-10 Intangible Losses

Cargo theft and pilferage losses in today's multimodal transportation system are ever present through the less visible impact of:

- Insurance claims.
- Administration of cargo theft claims.
- Delayed or lost sales for post exchanges, commissaries, class VI stores, etc.

■ Lost business by carriers.
■ Embargoes and interference with the flow of commerce.
■ Diversion of cargo.
■ Higher prices/freight rates increase loss of government revenue.
■ Reduced operational readiness of personnel, equipment, and supplies.

12-11 Carrier Protective Services

Protective services availabIe from a carrier are specifically described in the contract, tender, or tariff. The following protective services should be considered:

a. Exclusive useof vehicles (see paragraph 226, MTMR):

Reduces breaking of seals (appendix c, MTMTS PAM 55-4)
Total vehicle security.

b. Constant surveillance service (required by parpagraph 22660 2d, MTMR).

□ Overall shipments involving vehicles and commericaial carrier personnel.
□ Operation/procedures.

c. Bill of lading annotations.

d. Signature security service (SSS).

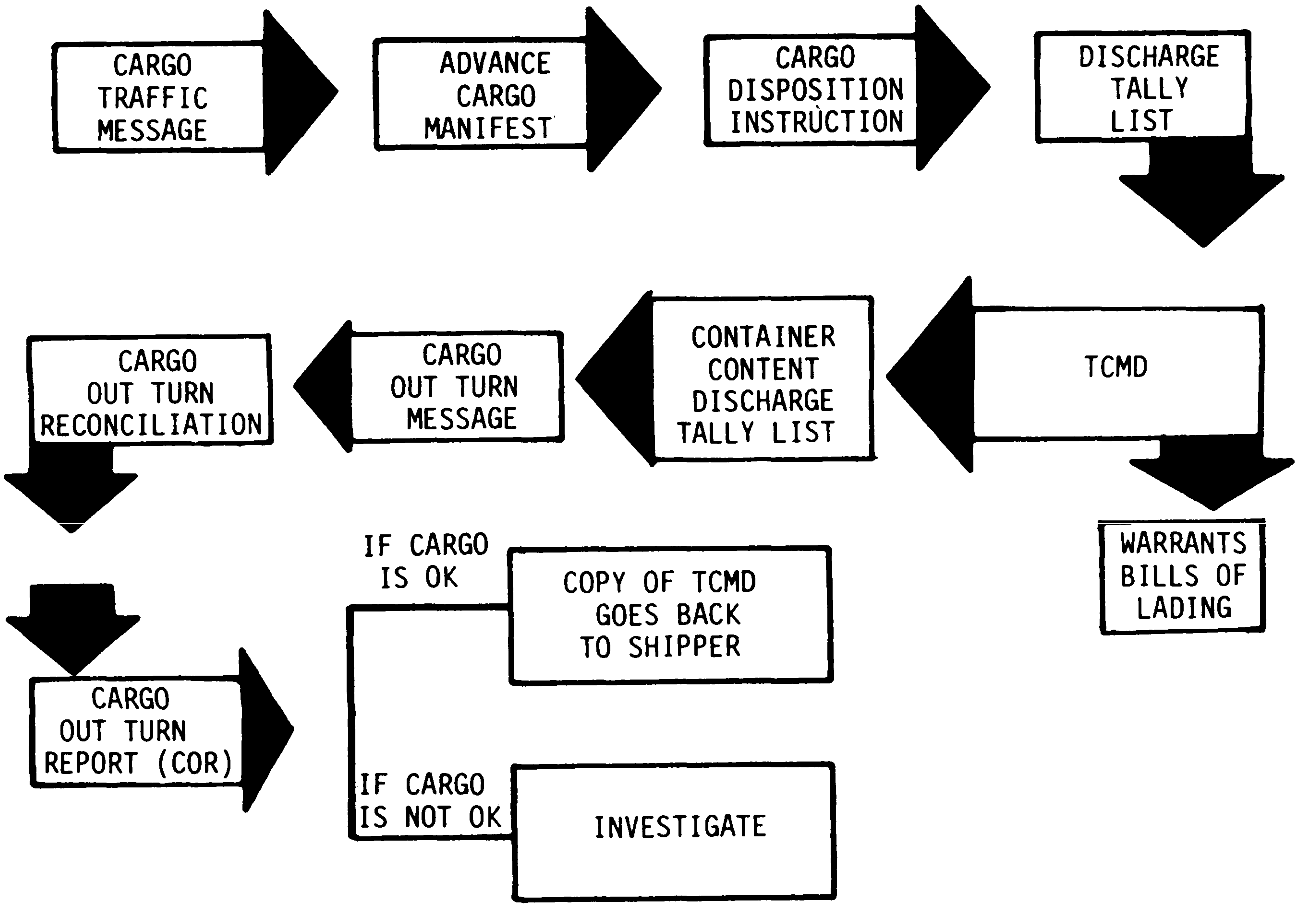


Figure 79—Steps in transportation process and corresponding audit trailpoints.

☐ Provides individual fixed responsibility for shipments.

☐ Provides tally record (DD Form 1907) and audit trail (figure 79).

e. Include dual driver protective service where constant vehicle attendance by two persons is provided.

f. Rail surveillance service provides hourly security checks of the rail car when it's not moving.

12-12 Protective Security Service (PSS)

PSS is a transportation security function of the Government involving contract shipments.

a. In addition to SSS (par. 12-11d), the PSS must insure that the transporting earner is a cleared carrier as defined in paragraph 22600, MTMR.

b. Shipment must be under constant surveillance of designated employees who are appropriately cleared.

c. DD Form 1907.

(1) Provided to the carrier by the shipper.

(2) Required for each person responsible for proper handling of the shipment (only one set of forms used/passed along with the shipment).

(3) Must accompany shipments requiring SSS.

(4) Required from air carrier personnel but not from flight crews or attendants. Commercial airlines use Form AC-10 in lieu of DD Form 1907, therefore, coordination to insure accuracy of records is a must.

(5) Carriers providing SSS must be able to trace a shipment in less than 24 hours.

12-13 Armed Guard Surveillance

a. This service provides armed guards to maintain constant and specific surveillance of shipments for which the service is requested.

b. A guard in this case is considered armed when he has a firearm and appropriate ammunition readily available for immediate use.

12-14 Unarmed Escort

Escort personnel must be cleared to the degree of classification required for the shipment. They must possess valid identification cards and must maintain constant surveillance over the shipment.

12-15 Routing Security Shipments

Managers and security personnel should consider the following prior to selecting a route for shipment:

- Threat by hostile elements or lone personnel.
- Value of shipment and required degree of security (by regulations).
- Identity of commodity.
- Strength of basic unit package.
- Total weight and number of pieces.
- Security capabilities of consignee and intermediate transshippers.
- Primary and alternate routes.
- Strength of transport container.
- Quality of service or claims record of the carrier.
- Cost of movement.

12-16 Sensitivity of Cargo

As indicated in paragraph 12-15, there is no simple solution to every routing problem. After considering all alternatives, sometimes imagination is still needed. For example, containers on a flatcar, over some rail routes, can be particularly vulnerable to pilferage. On the other hand, movement by motor is more costly and, even with protective measures, it too may require extra security. (See mode selection guide, appendix U, p. 493.) The solution usually is the use of special guards. However, where consignor and consignee have heavy lift capability, this more expensive solution (special guards) can be avoided by using rail and by loading containers in gondola cars. This arrangement permits substantial blocking of side doors and back doors. When butting to another container is not possible, additional protective measures such as intrusion detection devices and barbed wire might be required.

12-17 Protective Security Measures

a. Protective measures for shipments must be compatible with the threat.

b. Three types of protective measures are:

(1) Physical (containers, storage warehouses).

(2) Personnel (consignee, guards, etc.).

(3) Procedural (accounting, shipping, receiving, etc.).

c. Three degrees of cargo control are:

(1) Minimum-provided all cargo:

(2) Medium-provided:

- High-value cargo with a ready resale.
- Others as designated.

(3) Maximum-provided:

- Classified material.
- Small arms and ammunition.
- Other materials requiring strict control.

12-18 Packing Marking, And Addressing

From a security point of view, a packing list should be considered when packing, marking, and addressing merchandise for shipment. Preparation of a packing list is necessary on all shipments to assist the transportation officer in determining shortages. **Extremely close attention should be provided to packing list preparation when several shipments and pieces are consolidated.**

12-19 Alarm Devices During Shipment

a. Alarm devices have the basic function of providing a warning when a shipment has been moved from its proper location; or when the security being provided by the container or vehicle holding the shipment has been breached (such as opening container doors, or tampering with the shipment).

b. The devices used should:

(1) Augment other security measures.

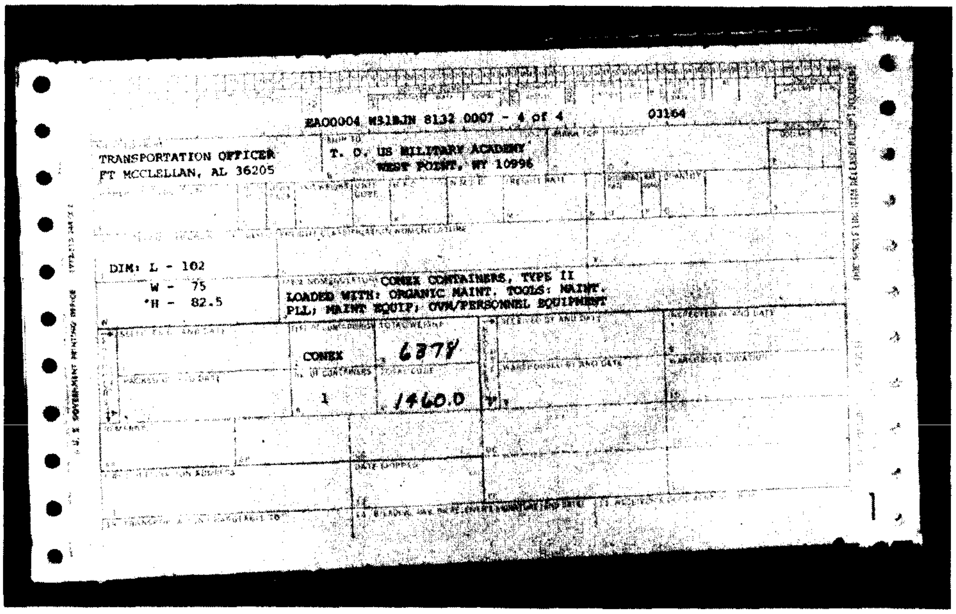
(2) Provide protection under unusual circumstances.

(3) Conserve manpower security resources.

c. Technically speaking, an alarm device is only that part of an intrusion detection system that sounds the alarm. Actually there are **three basic parts:**

(1) Sensor to detect noise, presence, or movement.

(2) Wire or transmitter to send the sensor signal to a receiver/annunciator.



TRANSPORTATION OFFICER
FT MCCLELLAN, AL 36205

T. O. US MILITARY ACADEMY
WEST POINT, NY 10996

DIM: L - 102
W - 75
H - 82.5

CONEX CONTAINERS, TYPE II
LOADED WITH: ORGANIC MAINT. TOOLS: MAINT.
PLL; MAINT EQUIP; OVM/PERSONNEL EQUIPMENT

CONEX 6378

1 1460.0

Figure 80—Packing lists offer opportunities for pilferage—when not used and when altered or improperly prepared.

(3) Receiver/annunciator to display or emit a notification (as a light, sound, or switch to trigger another device), indicating the situation detected by the sensor.

d. Most intrusion detection systems are designed for fixed installations and do not lend themselves to shipments. A few have the primary purpose of detecting anyone moving a shipment or entering a transport container or vehicle. Alarm devices suitable for ship ment use and available from commercial sources include:

- **Entry alarms.** Similar to the common house burglar alarm, these are built to operate on a small battery and emit a mind-wrenching sound, which can be.felt as well as heard.
- **Movement alarms.** These operate on the principle of a radio; that is a transmitter and a receiver.
- **Small motion sensors** easily attached to a container or vehicle door transmit a coded radio frequency signal when the door is opened or the container is moved. The signal is picked up by a receiver, which notifies a guard.
- . A **tarpaulin,** constructed of heavy waterproof fabric with **built-in motion sensors,** operates on the same principle. Any movement of materials from under its cover causes transmission of a radio signal.
- **Application of devices.** The security officer must be consulted in applying any device.

12-20 Use of Seals

The following guidelines must be met in using seals in transportation security:

- Show if the integrity of a shipment has been compromised.
- Maybe used as a seal-lock or cable seal. (A lock is not necessarily a seal, and a seal is not necessarily a lock.) (See figure 81.)
- Unless funds and time are unlimited, there is no particular seal, lock, or combination suitable for every situation. For example, a high-grade lock on a weak container hasp is a

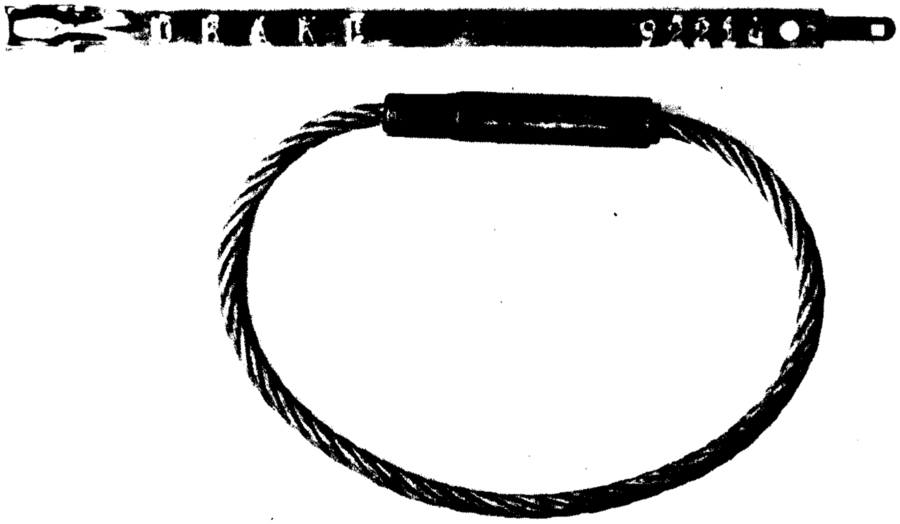


Figure 81—A seal is not a lock and a lock is not a seal.

waste of money and a high grade seal is of no value on an easily removed door.

☐ Strict seal accountability is a must, and accountability should be constant.

☐ Accountability starts with the manufacturer and ends with seal destruction.

☐ Seals, to be effective, must meet two basic requirements —construction specifications and accountability.

12-21 Seal Construction Specifications

a. Durability. A seal must be strong enough to prevent accidental breakage during normal use.

b. Design. The design must be sufficiently complex to make unauthorized manufacture of a replacement seal difficult.

c. Tamperproof. The seal should provide readily visible evidence of tampering and preclude reconstruction after the seal is closed; that is, a seal should be constructed so as to make simulated locking difficult.

d. Individually identifiable. Identification must be accomplished by embossing serial numbers and owner identification on each seal.

12-22 Seal Accountability

Each seal should be strictly accounted for from manufacture to the time of application. Seal custodians, users, users' subordinates authorized to apply seals, and seal removers must be appointed in writing. These appointments should be kept to a minimum. Procedures listed below must be followed:

- All seals must be ordered or purchased from manufacturer by the same office of an organization and must be recorded serially in a log by the seal custodian.

- Until issued to users, all seals must be safeguarded in a suitable locked metal container, limiting access, under supervision of the custodian, in a manner that will

prevent unauthorized substitution or illegal use of seals.

12-23 Issuing Seals to Users

a. Custodians must issue seals to users, obtain a receipt, and record issuance by number.

b. Each seal user must maintain a log showing numbers of all seals and the date received.

c. Each user and his employees authorized to apply seals in a terminal must sign or initial for the seals, by number, and after applying seals in a terminal, prepare a seal application log, showing date and trailer number to which applied.

12-24 Seal Application And Verification

a. Record of application—seal numbers must be entered in the designated place on pertinent transportation documents; such as bills of lading, manifests, gate passes, and in users' seal application logs.

b. Time of application— trailers must be sealed as soon as the load is closed out (complete). Roll-up type doors must be sealed by the checker at the dock. Swing out doors must be sealed by the person pulling the unit away from the dock as soon as the unit is far enough away for the doors to be closed.

c. Verification— seals must be examined and verified at every stop; such as terminal exits and entrances, docks, transfer points, and road stops for truck and driver services.

(1) The gate guard must check the seal number against the gate pass and shipping documents and note seal numbers, along with the trailer and tractor number, on his gate log.

(2) Persons receiving sealed shipments or equipment must examine the seal and record the number on the receipt.

(3) Whenever a seal is removed, broken, or suspected of having been compromised, the following actions must be accomplished:

(a) Record pertinent information:

- Date and time seal was removed, broken, or discovered broken, etc.
- By whom, organization, name.
- Circumstances/justification for breaking the seal.
- New seal number, if applied (new seal must be same type).
- Person resealing.
- Witness.

(b) Make proper disposition of broken seals.

■ Retained until it is determined whether the shipment contained discrepancies.

■ If there were none, the seal should be destroyed.

■ If any discrepancy is found, the broken seal must be sent to the security manager.

■ If shipment contains classified information, material, or equipment, the following actions, as a minimum, must be immediately initiated:

- Secure the area.
- Position security guards.
- Notify the commander.
- Contact local support MI office.
- Conduct immediate inventory by authorized personnel.

12-25 Breaking Seals And The Law

Title 18, US Code, Section 2117, states: *"Whoever breaks the seal or lock of any railway car, vessel, aircraft, motor truck, wagon or other vehicle...containing interstate or foreign shipments of freight or express, or other property, or enters any such vehicle... with intent in either case to commit larceny therein, shall be fined not more than $5,000, or imprisoned not more than 10 years, or both..."*

12-26 Legal Considerations For Guards/Escorts

a. The duty of a common carrier of property is to provide all reasonable and necessary facilities for safe and efficient transportation of such goods as it holds itself out to the public as engaged in carrying.

(1) This includes the duty to carry such goods safely and to exercise the care required to protect. them from loss or injury during transportation.

(2) These duties are imposed by the common law and statute. For this reason, horn the time goods are turned over to a carrier for transportation until final delivery has been made, a carrier's liability is that of an insurer, with certain exceptions (act of God, act of the public enemy, act of the shipper, etc.).

(3) In keeping with the duties and liabilities imposed by law, a carrier, as a bailee of goods, will necessarily exercise full control and custody over the lading. Accordingly, while the goods are in transit, the carrier, not the shipper, is responsible for proper care of the goods.

b. At the same time, the shipper retains the legal right during the time the goods are in transit to have his consignment interrupted, withheld, reconsigned, or diverted at any intermediate point.

(1) While this is a right afforded the shipper under law, the services rendered by the carrier in connection therewith are supplementary services which the carrier is obligated to provide and may collect for.

(2) These services and charges, as well as the terms and conditions under which the shipper's right to be exercised, are, in effect, a contractual matter to be established and governed by the carrier's tariff or tender.

c. Such supplementary services are ordered by the shipper or someone authorized to act in his behalf. Insofar as the shipment of Government property by commercial carriers is concerned, the Government, as a shipper, acts through duly appointed transportation officers or their authorized representatives. Presently, only a transportation officer or his authorized representative may exercise such responsibilities. The assigned duties and responsibilities of armed military escorts are limited to maintenance of security over the property being transported and do not in any way extend to the ordering of transportation services, or changes thereto, that might be required in any emergency.

d. While the right of the shipper to have his consignment interrupted, diverted, or rerouted is based on law, the carrying of escorts or guards provided by shippers to accompany shipments is permissive on the part of the earner, and, where authorized, is a matter of contract to be spelled out in the carrier's tariff or tender. In this connection, the inclusion of annotations on bills of lading setting forth a requirement for escorts and stating their responsibilities would be ineffective unless provisions are first spelled out in the carrier's tariff or tender.

e. A carrier used by a shipper for transportation of special cargo requiring an escort may be a contract carrier or a common carrier

providing services under a commercial tariff or a Section 22 tender. Common carriers providing transportation services for the Government generally provide such services under Section 22 tenders. The Section 22 tender, as a commercial tariff, sets forth services the carrier will perform, applicable charges, and conditions of shipment. In effect, it is the governing contract. It usually contains the following provisions relative to armed security guards:

> *When requested by the shipper, an armed security guard (furnished by the military accompanying the shipment) will be permitted to ride in the carrier's vehicle. This guard will be responsible for the security of the shipment from origin to final destination but will not be responsible in any way for the operation of the vehicle or the route to be followed.*

f. Authority to direct or otherwise control movement of the cargo in question will be granted to an escort, provided appropriate provisions are included in the carrier's tariff or tender, and the escort is duly appointed to act as the transportation officer's representative for the desired purposes.

12-27 Guards/Escort Instructions

Instructions and operating procedures. Specific written instructions and operating procedures must be furnished escort/guards and will include, but not necessarily be limited to, the following:

a. General unclassified outline of the mission.

b. Name and address of person(s), including alternate(s), to whom classified matter is to be delivered.

c. Receipting procedures.

d. Means of transportation and route to be used.

e. Duties of each escort during movement, stops en route, and during loading and unloading operations.

f. Emergency and communication procedures.

12-28 Escort Functions

Escorts assigned for the protection of shipments must adhere to the following guidelines:

a. Conduct themselves in such a manner that the security of matter entrusted to them will not be prejudiced through carelessness, inadvertence, or lack of vigilence. Intoxicants or drugs that may impair their judgment may not be used by escorts while assigned to a security shipment.

b. Possess identification cards and carry them at all times while having custody of security shipments. These cards must be safeguarded, and the loss of a card must be reported immediately to the security supervisor.

c. Carry packages on his person, or in hand-earned containers, until delivered to consignee whenever practicable.

d. Provide continuous observation of the shipment, vehicle, or container and be in a physical position to exercise direct security controls over the material.

e. Maintain liaison, as required, with train crews, airport and other transportation personnel, special police, and law enforcement agencies, as appropriate.

f. Maintain continuous vigilance when escorting security shipments for the presence of conditions or situations that might threaten the security of the cargo; take action as circumstances might require to avoid interference with continuous safe passage of the vehicle; and check seals and locks at each stop where time permits.

g. When escorting shipment by aircraft, the escort will not enplane until the cargo area is secured. The escort should preferably be the first person to deplane in order to observe the opening of the cargo area. Advance arrangements with the airline are required.

h. Notify the consignor by the fastest means available if there is an unforeseen delay en route, an alternate route is used, or if an emergency occurs. If appropriate and if the security of the shipment is involved, notify the nearest office of the Federal Bureau of Investigation (FBI).

12-29 Use of Firearms (See AR 190-28)

The responsible commander may require the use of armed guards for protection of materiel under his jurisdiction. Military and civil service personnel are authorized to be armed as deemed necessary without regard to state laws concerning weapons, as long as the individual remains within the scope of his orders on bearing and using arms. Such personnel will comply with the provisions of federal law when applicable. Commercial carrier and contractor personnel bearing arms in the accomplishment of a shipment do so under the authority and control of both state and Federal laws that apply. The commercial earner or contractor is responsible for arranging any necessary permits in this regard.

Ordinarily, classified shipments do not require the arming of escorts.

12-30 Guards For Oversea Shipments

When cargo guards arrive at a terminal or port to begin escorting a ship ment, the following general instructions apply:

a. Senior members of the guard must report to the officer in charge of cargo operations for any special instructions. In general, responsibilities of the cargo security officer (may be the senior guard member) begin upon arrival at the loading terminal and terminate when relieved by appropriate authority at the port of debarkation. While the shipment is in the terminal, and provided adequate facilities exist to safeguard the cargo, temporary custody of shipment maybe taken by the terminal.

b. A joint inspection of the condition of the following items must be made by the senior member of the classified cargo guards and a representative of the terminal commander before and after each operation:

(1) Quarters provided aboard ship or other carrier as to the cleanliness and adequacy for personal occupancy.

(2) Railroad escort car, etc., prior to its being vacated by the guard(s).

c. If possible, a conference is held with the master of the vessel or his representative, senior guard member, and loading terminal personnel prior to loading classified cargo, to insure complete understanding of all responsibilities involved.

d. Appropriate receipts covering cargo and/or understanding of instruction or relief of responsibilities must be executed or secured by the loading terminal from the senior guard member.

e. While aboard ship, cargo guards must:

(1) Conduct inspections upon relief of each guard and during tours of duty of cargo spaces containing classified cargo, for condition of materiel (if visible), signs of tampering, or pilferage.

(2) Maintain an inspection log, noting results of each inspection.

(3) Be immediately responsible to the master of the vessel. Coordinate duties and

inspections with a ship's officer in a manner that will not interfere with operation of the vessel. Responsibilities aboard the vessel must be confined to safeguarding the classified cargo.

f. If damage to cargo or other irregularities are noted, immediately report the facts and circumstances to the master of the vessel, and confirm the irregularity in writing. Copies of such reports will be attached to the narrative voyage report furnished to the commander of the outloading terminal and the oversea discharge terminal.

g. Photos of damaged or pilfered containers, if required, will be taken by the commander of the discharge terminal with permission of the master of the vessel.

12-31 Sensitive Shipments

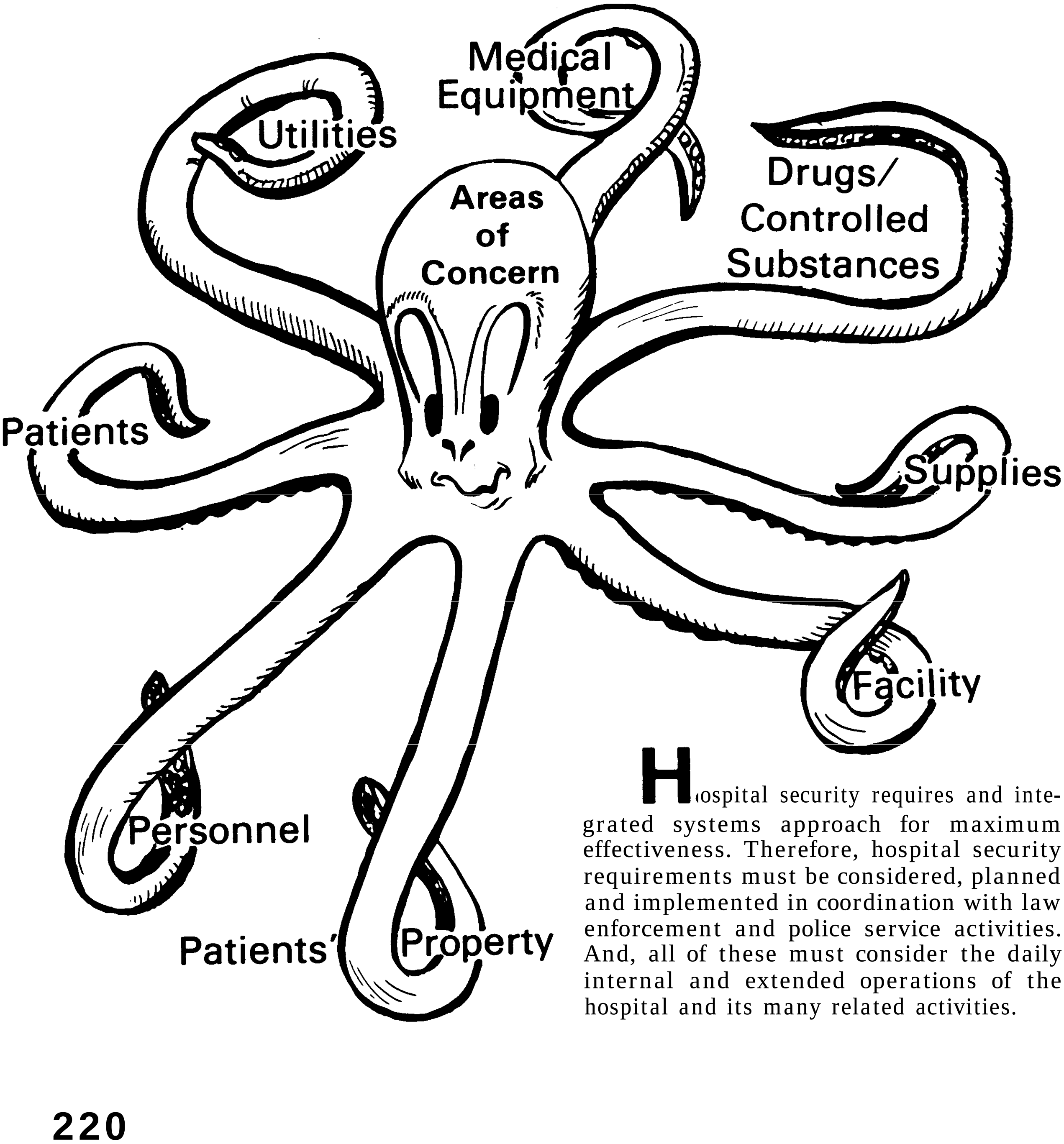
Shipments involving weapons, ammunition, explosives, and special weapons and chemicals **require special security measures in addition to those discussed in this chapter.** These additional requirements are explained in the following Army regulations:

(1) ARs 190-11 and 190-49 for weapons, ammunition, and explosives.

(2) ARs 50-5, 50-6, and 55-228 for special weapons and chemicals.

Chapter 13

Hospital Security



Hospital security requires and integrated systems approach for maximum effectiveness. Therefore, hospital security requirements must be considered, planned and implemented in coordination with law enforcement and police service activities. And, all of these must consider the daily internal and extended operations of the hospital and its many related activities.

Responsibilities

13-1 Security Coverage

a. Effective hospital security encompasses all of the following

- Installation hospitals
- Medical centers (MEDCENS)
- Medical department activities (MEDDAC clinics and dispensaries)
- Special mission activities.

b. Each MEDCEN or MEDDAC is usually composed of several fictional activities which must be considered when establishing security measures to prevent pilferage and to protect sensitive items, equipment, structures, and key personnel. These activities include:

- Dental activities.
- Veterinary activities.
- Community mental health activities.
- Health and environment activities.
- Pharmacy or any controlled medical substances storage facilities.
- Medical supply facilities.
- Hospital treatment and care facility.
- Medical warehouse storage facilities.

13-2 Provost Marshal/Security Officer

a. The Health Services Command (HSC) director of security and subordinate MEDCEN/MEDDAC provost marshals/security officers must direct the command'sd's crime prevention and hospital security program. The responsibilities of these positions include the following:

- ❑ Develops policy and standards for crime prevention and hospital security.
- ❑ Performs onsite inspections.
- ❑ Guides related law enforcement and police service activities within the health care system.
- ❑ Advises on use of military police.
- ❑ Maintains crime trend statistical data.
- ❑ Performs liaison with law enforcement and security elements of higher, lateral, and subordinate headquarters, and with civil and other Federal law enforcement personnel.

b. To insure proper security, it is essential that the provost marshal/security officer be included as a member of construction review boards and therapeutic agent boards.

c. He provides direct input to contingency planning for

- Field operations and disasters.
- Bomb threat/natural disasters, etc.
- Physical security on what, when, where, and how to best provide it.
- Measures (what the individual should do).
- Techniques (how devices are setup, placed, etc.).
- Devices (what to look for).

d. The provost marshal/security officer is also responsible for circulation control of vehicles and individuals and for police service support as required.

13-3 Circulation Control

Controlling the movement of vehicles and people is a **continuous consideration** in hospital security. Effective circulation control includes the following:

a. Routing controls.

(1) Establish vehicle traffic patterns.

(2) Designate pedestrian movement patterns.

(3) Insure proper use of information signs and services.

(4) Direct procedures for enforcement.

(5) Establish visitor parking areas.

b. Special controls.

(1) Patient parking areas.
(2) Hospital staff parking areas.
(3) Handicapped person(s) parking areas.
(4) Emergency vehicle entrance/exits (enforced by MPs).
(5) Emergency vehicle parking areas.
(6) Equipment/supplies offloading.
(7) Taxi/bus pickup points.
(8) Fire department vehicle parking near water plugs (enforced by MPs).
(9) Law enforcement vehicle parking.

c. Reporting procedures for suspicious or unidentified persons and activities.

d. Chapter 4 has more information on personnel movement control.

13-4 Security Lighting

a. Routine use.

(1) Within medical treatment facility.

(2) Adjacent to medical treatment facility.

(3) Along all well-traveled foot paths where possible.

b. Special use.

(1) Prevent/reduce crimes.

(2) Prevent/reduce vehicular and pedestrian accidents.

(3) Assist in emergency activities.

(4) Accommodate nighttime circulation pattern, or vice versa.

(5) Entrances to critical areas, sensitive areas, or other access points.

c. Chapter 6, Protective Lighting, contains more specifics.

13-5 Use of Dogs

a. Patrol and marihuana dogs.

(1) Use only with specific permission of medical commander.

(2) Detect and prevent unauthorized drugs from entering facility.

(3) Emphasis on dog use should be directed toward entrances to neuropsychiatric and detoxification wards.

b. Sentry dogs.

- Used only outside the medical treatment facility.
- In high risk areas.
- Near areas for storage of supplies and equipment.

13-6 Key and Lock Control

AR 190-50, Section II, sets policy for key and lock control. Briefly, hospital requirements in this area are:

a. Continual emphasis.

b. Establishment and implementation of an aggressive plan.

c. Use of safeguards for

■ Controlled substances (see the Security Inspection Checklist below).

Physical Security Inspection Checklist
Narcotics And Controlled Drugs (AR 190-50)

- □ Does the location of the room/area afford adequate protection?
- □ Is the room/building that houses the narcotics of permanent construction?
- □ Are bulk narcotics/controlled drugs stored in a vault or similar protective storage?
- □ Is there an authorized narcotics cabinet or chest (hospital ward)?
- □ Is the vault, safe, or cabinet kept securely locked when not in use?
- □ Are responsible persons in close vicinity to assure protection?
- □ If narcotics are stored in a small movable safe or the like, is the safe adequately secured to a permanent part of the storage room or building?
- □ Is the register secured and available only to authorized personnel?
- □ Is an intrusion detection device or system installed, working, and tested weekly?

- High cost medical equipment.
- Highly pilferable supplies.
- Mission essential areas.
- Vulnerable areas.
- Medical supply storage areas.

d. Chapter 8, Locking Systems, has more details on lock and key control.

13-7 Intrusion Detection Systems (IDS)

a. Regular installation and special hi-weekly testing of IDS/duress alarms should be accomplished for medical treatment facilities and for medical supply storage activities.

b. Alarm annunciation at the military police station is a necessity, to provide continuous monitoring capability and an armed police force response.

c. See chapter 7, Intrusion Detection Systems for IDS details, and AR 190-50, Section II for DA policy.

13-8 Personnel Screening

Because of the vulnerability to criminal activity of medical property and that of patients, military personnel and civilian employees must be adequately screened for hospital duty. This also applies to other categories of facilit y workers, such as contractor employees.

Minimum screening must include a local military and civilian police records check and an NCIC check.

Reclassification and discharge proceedings are processed on persons involved in criminal activity. This also applies to high risk military and civilian employees.

13-9 Material Control

a. Management and control of medical material is necessary regardless of the number of times it is exchanged. The following items require special security and accountability:

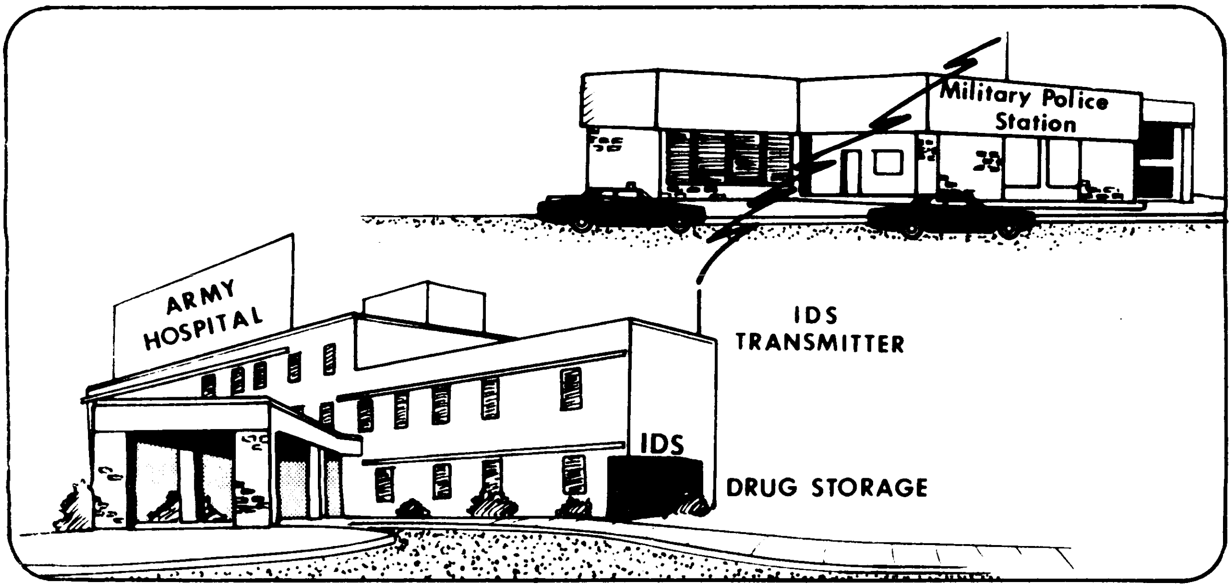


Figure 82— The IDS must alert the MP station.

- ☐ Controlled substances
- ☐ Stored hospital linens
- ☐ Expensive medical equipment
- ☐ Money and valuables
- ☐ Other sensitive items.

b. Store sensitive and accountable items away from the mainstream of heavy foot traffic to assist in detecting removal.

c. Equipment and medical substance disposal must meet these guidelines:

(1) Equipment will be disposed of IAW established regulations and directives.

(2) Medical substance IAW ARs 40-2, 40-61, and TB Med 291.

(3) Disposal must be supervised by appropriate custodial personnel.

(4) Including foodstuffs.

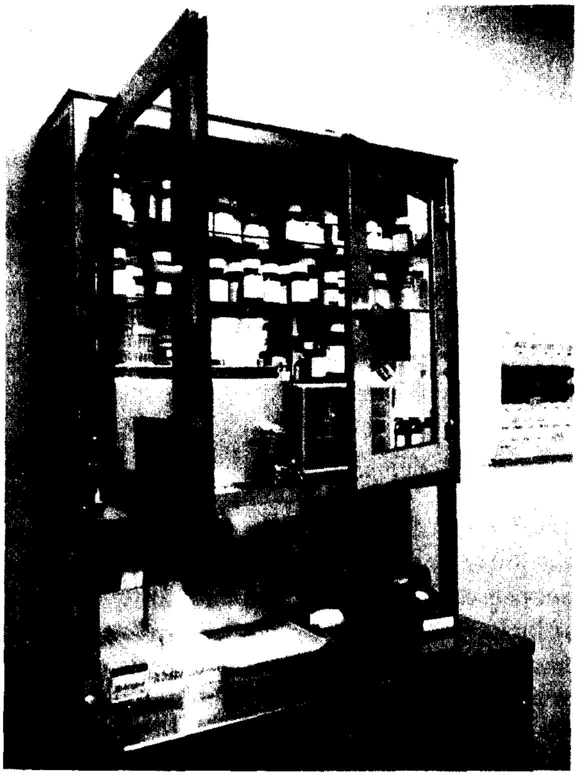


Figure 83—Unlocked medicine cabinets invite theft / pilferage.

13-10 Controlled Substance and Medically Sensitive Items

a. Require special security and handling to prevent loss and public injury (par. 2-5, AR 190-50). This includes:

- ■ Drugs
- ■ Precious metals
- ■ Radioactive medical materiel
- ■ Needles and syringes.

b. Consumption of drugs must be by authorized prescription.

c. See checklist for narcotics and controlled drugs on page 223.

13-11 Intransit Security Of Controlled Medical Substances And Other Sensitive Items

These items must be protected from unauthorized possession, use, and theft. The guiding regulation is AR 40-61.

13-12 Protection of Individuals

a. Special consideration must go to patients, prisoners, visitors, and the hospital staff.

b. Patient categories that must be considered:

(1) VIP—military and civilian.

(2) Active duty personnel.

(3) Dependents (check ID cards with hospital cards).

(4) Retirees of all services.

13-13 Patients' Personal Property and Valuables

- Retainable money for comfort and convenience items.
- The secured patients' trust fund.
- Valuables left on the ward as gifts, etc.
- Military pay.
- Other personal items (radios, tapes, clothing, etc.).

13-14 Medical Treatment

Records of patient treatment must not be available to the visiting public. Nor will the information contained therein be released during telephone conversations. These restrictions are covered by the Right To Privacy Act, DA guidelines, and HSC directives on the subject. Personnel awareness briefings should be held concerning criticality of records to the total individual.

Records will be released under signature only. Those involving official investigations must be released IAW published directives. When MPs desire private medical information on individuals for official use, they must request it on DA Form 4254-R. Other Federal law enforcement personnel must make their requests according to paragraph 4(b), AR 40-42.

13-15 Emergency Treatment Facilities

Because the medical treatment staff is extremely occupied with emergency patients, emergency rooms and triage areas pose special security problems regarding patients' personal property and valuables and Government property (weapons, ammunition, etc.).

Security problems are compounded by the disruptive effects of

- Friends and relatives
- Other patients (able/disabled)
- Children
- Investigating police
- News media
- Chain of command personnel.

These areas should be sealed off to all except selected medical staff personnel. The areas may be controlled by military police under special circumstances. Information points should be designated and identified by signs.

13-16 Security Checks

a. Military police, security police or interior guards must conduct periodic checks each shift of isolated structures containing medical items and equipment. HSC security staff duty officers, medical, and unit personnel may inspect facilities within hospitals, RDT&E complexes and structures, and other medical facilities.

b. These checks should be conducted at irregular intervals. Increase frequency during hours of darkness or periods of limited visibility, and on weekends and holidays. Suspected loss, illegal entry, theft, open or unlocked facilities or containers, or suspicious incidents must be immediately reported to the nearest military police.

c. Security for bulk storage facilities, pharmacy storage, medical treatment facilities, TDT&E laboratory facilities must be secured IAW AR 190-50.

Security Standards and Structural Applicability

Section III

13-17 See AR 190-50 For Security Standards And Structural Applicability Of Controlled Medical Items

Emergency Utilities System

Section IV

13-18 Separate Protection

Protection of utilities is a vital effort of security police and must be separated from hospital materials protection. Utilities include the primary power source and the alternate power source. As a minimum, the utilities have an impact on the following areas designated as limited access areas:

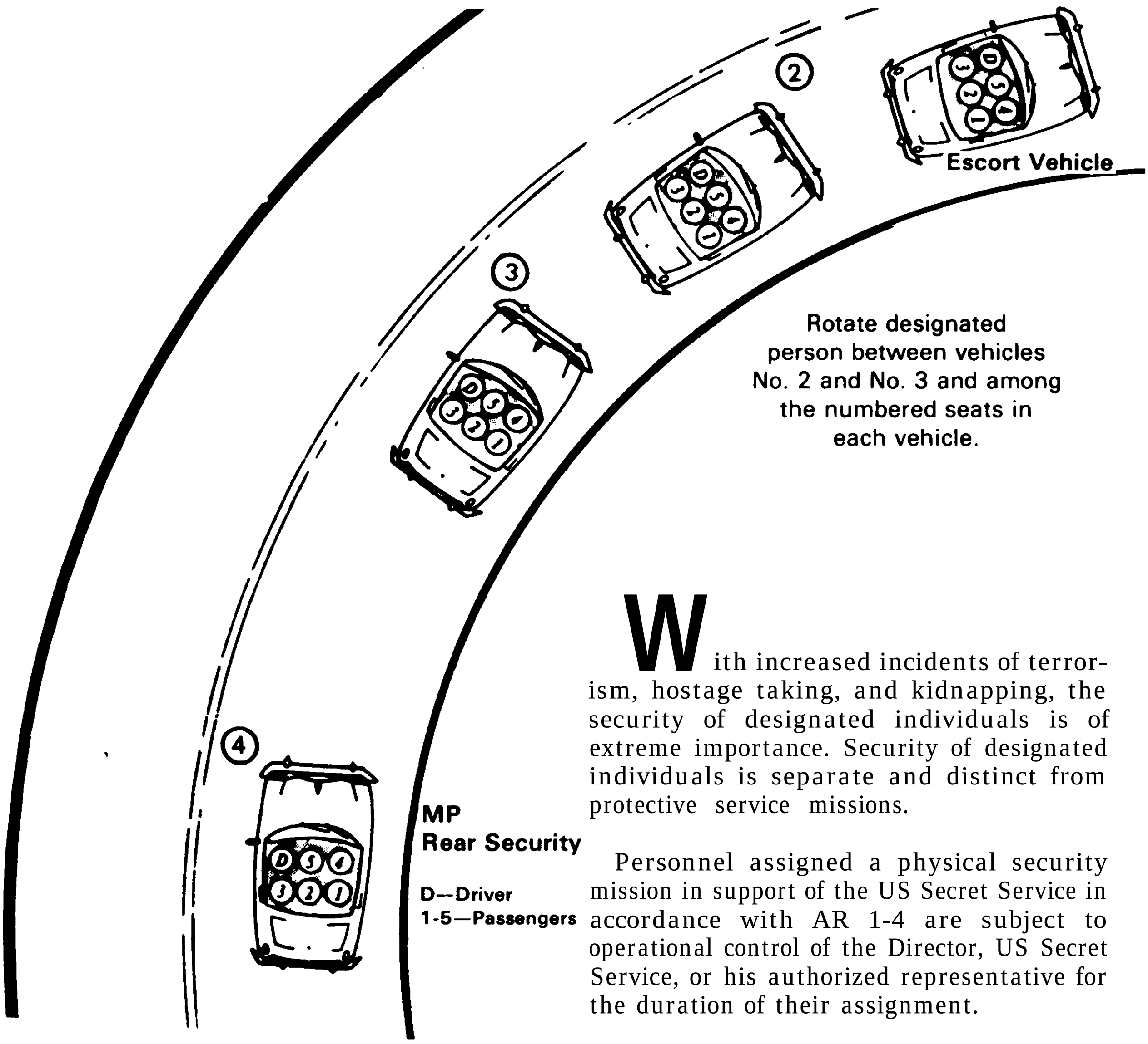
+ Emergency treatment facilities
+ Operating room(s)
+ Intensive or special care wards
+ Pharmacies
+ Food preparation
+ Emergency operation center (EOC)
+ Communications and control centers

13-19 Utility Services

Protection of the following vital areas must be coordinated and integrated into the installation provost marshal contingency plans:

- ☐ Water
- ☐ Natural gas
- ☐ Fuel oil
- ☐ Electricity/backup generators
- ☐ Telephone
- ☐ Heating
- ☐ Air conditioning
- ☐ Air filtration units.

Personal Security of Designated Individuals



With increased incidents of terrorism, hostage taking, and kidnapping, the security of designated individuals is of extreme importance. Security of designated individuals is separate and distinct from protective service missions.

Personnel assigned a physical security mission in support of the US Secret Service in accordance with AR 1-4 are subject to operational control of the Director, US Secret Service, or his authorized representative for the duration of their assignment.

Since the problems of personal security vary so greatly with each individual case in terms of potential hazards and threats, political and sociological considerations, geography, environment, mode of transportation, etc., the preparation of a comprehensive SOP is virtually impossible. There are, however, basic factors that must be considered which can be applied to all situations regarding personal security.

Authority and Mission — Section I

14-1 Authority

The authority to secure designated individuals is outlined in the following Army regulations:

- AR 1-4
- AR 10-23
- AR 190-10
- AR 190-30
- AR 210-10

a. AR 1-4 prescribes support to the US Secret Service and specifies that the director of this agency or his authorized representative will have operational control over Army personnel selected for this support.

b. AR 10-23 pertains to the US Army Criminal Investigation Command. The principles, procedures, and organizational concepts of personal security are provided for law enforcement/security personnel of installations/activities.

c. AR 190-10 refers to the protection of dignitaries not listed in AR 1-4 or 10-23.

d. AR 190-30 pertains to the employment of military police investigators in the security of persons under Army control.

e. AR 210-10 states that the security of an installation is the responsibility of its commander.

14-2 Mission Accomplishment—Delegating Responsibility

The installation commander must designate a physical security officer IAW AR 190-13. This duty position will normally be in the provost marshal security office.

a. Personal security of designated individuals is within the scope of physical security responsibilities. The skills and other knowledge of military police/security personnel give them the background, most easily adaptable to personal security tasks.

b. The following organizational concepts are essential to this mission:

(1) Operational personal security teams.
(2) Designation of an officer in charge.

The purpose of a security protection plan is to minimize the chances of success of any contemplated attack.

14-3 Security Principles

a. Every phase of security must be carefully considered in advance, to include the importance of the protected person, political attitude of the population, obstacles involved, means of transportation, and duration of the security mission.

b. Physical protection should consist of a series of protective cordons, each complete in itself. These protective cordons may be composed of security personnel or physical barriers, or a combination of both. An example of this type of security is the protection established around a house desig nated as a residence for the dignitary. A protective cordon may include these steps:

(1) A number of walking patrols around the grounds to establish a protective cordon.

(2) A series of fixed posts at entrances would provide another form of cordon.

(3) Security personnel stationed within the house form the third echelon of protection (security in depth).

c. Central direction and unity of effort are of special importance because of the nature of this assignment. The officer in charge should be given full responsibility for all phases of the security mission, such as coordination:

(1) Close coordination must be established with all local military and civilian authorities. On an installation, for example, coordination must be accomplished with the headquarters commandant, transportation officer, intelligence officer, and others as applicable. Civilian authorities will include police and other interested city, county, state, or comparable officials.

(2) The agencies responsible for each phase of the security plan must be clearly defined. Arrangements should be made for local civil police to control local inhabitants. All available intelligence channels should be used to obtain information of potential danger areas, persons, or groups.

(3) Much of this coordination can best be accomplished by an advance party after the official itinerary is received.

d. Personnel selected for the security detail should be mature, experienced, and outstanding in physical appearance and bearing. Personnel assigned to a security detail involving regular or frequent contact with the President, or access to Presidential facilities, are selected in accordance with special procedures prescribed in AR 614-3.

e. Technical assistance. In many of the activities and procedures discussed in this chapter, the assistance of qualified technical personnel will be required. For example, inspections of buildings will require Engineer assistance; vehicles, aircraft, and boats

should be inspected by trained mechanics. Other technical assistance should be obtained as necessary.

f. Continuing personal security operations. Certain MP and CID personnel/units have continuing personal security assignments to designated persons and continuing responsibility for their security. For these personnel/units, all of the responsibilities and tasks described in terms of visits and tasks in this chapter are continuing responsibilities and tasks. Ordinarily, these personnel/units have no other MP or CID responsibilities, and concentrate their total effort on their personal security operations. For the CID protective service responsibilities, see USACIDC Pam 195-1.

g. Routes and means of transportation to be used by the protected person should not be publicized. In many instances this is not possible. The itinerary, more often than not, receives wide publication. It may be necessary that he address public audiences, accept invitations to local civilian functions and receive delegations at railway stations and airports. Careful scrutiny of the normal itinerary will reveal many details that need not be made public. Routes to and from announced appointments usually need not be revealed. If a series of appointments is scheduled for a particular location, routes should be varied. No publicity should be given concerning the mission except that released by the information officer. Maintaining secrecy on the movements of the dignitary is one of the most effective means of minimizing the opportunity for attack.

14-4 Contingency Planning

Security planning should be flexible. Weather conditions and mechanical failures (including failure of lighting systems) are two ever-present potential hazards. The unexpected arrival of large numbers of visitors is another situation frequently encountered. Last-minute changes in the schedule of events occur routinely. The security plan must be sufficiently fluid to cover these and man y more eventualities, all of which present hazards.

a. An excellent format for preparation of a protective plan is the standard operation order in FM 101-5.

Requirements of the order are:

- Mission
- Concept of operation
- Coordination and liaison
- Itinerary areas-of interest
- Personnel and equipment requirements
- Cooperation
- Communication
- Logistical support
- Public relations
- Emergency information.
- Command and control.

b. The order should be in writing and produced in sufficient copies to be staffed with those officers with whom coordination is necessary. Length of the order will depend upon the size of the mission performed.

c. Only key personnel need a complete copy, but all protective personnel are given an orientation on the contents of the order and should be familiar with the whole operation. Each participant commits the requirements of his specific mission to memory. For this reason the order contains detailed instructions for each post and mission. These instructions must be simple to understand and easy to execute.

d. The itinerary and other information pertaining to the travel of a person, which is often attached as an annex may, under certain conditions, be classified in accordance with AR 380-5. Sufficient time must be allowed for dissemination of travel information to permit suitable security measures to be taken. The key to successful accomplishment of a security mission is detailed continuous planning and careful selection, training, and use of personnel.

e. In his planning, as well as in the execution of his mission the officer in charge should use the guidance furnished in other portions of this manual and other publications, adapted to his requirement.

f. FMs 19-15 and 19-25 provide valuable guidance in the areas of crowd control and traffic control, respectively. TC 19-17, Defensive Driving for Military Police, provides information on the proper techniques of operating a sedan at speeds higher than normal. All of these publications should be studied and used by the officer in charge.

14-5 Mission Orientation

An orientation should be conducted by the officer in charge of the protection plan, during which he explains filly the content of the plan. Examples of topics to be emphasized are:

a. Conduct and Demeanor of Security Personnel.

(1) Military police assigned to these duties are selected on the basis of their appearance, alertness, and intelligence, as well as their ability to act quickly and correctly in unforeseen circumstances (chapter 9). They are informed that no risks are taken with the safety and well-being of important persons. Protective personnel, to perform their mission efficiently, must understand the terminology peculiar to an assignment of this type. For example, a personal security guard mission may require a single bodyguard, a security guard unit or an escort unit.

(a) The mission may incIude direct or indirect protection or escort duty. Direct protection is open and obvious; indirect is generally a surveillance measure. The security guard unit may operate as an interior guard and may consist of one or more men stationed at fixed posts. Military police should know the identity of each individual in the party of a protected official.

(b) The attitude of the protected person must be estimated by the military police officer. In some instances the presence of security personnel is unpleasant to a dignitary. This is understandable in view of the lack of privacy inherent in personal security missions.

(c) Security personnel must be aware of this natural reaction, actually anticipate it, and adhere to strict policies of nonirritating conduct. In the initial planning stages, all potential embarrassment should be avoided. It is normally good policy to avoid direct contact with the dignitary on details of arrangements. The officer in charge should coordinate with a member of the official party who is designated for this purpose.

(2) When the protected person ignores measures taken for his protection, military police continue to perform their duties as directed. When appropriate, the officer in charge offers suggestions tactfully.

(a) Enforcement power over the security of the protected person is exercised by the chief of the escort only, and then only with caution and diplomacy.

(b) Any violation of security measures by any member of the party of the protected person is brought to the attention of the chief of the escort or guard. The military police officer insures that guards comply with every detail of their instructions.

(3) Restrictions on the circulation of individuals should be strictly enforced. Before any person is allowed to approach the dignitary or his effects, the person is checked carefully for identification and the authority for his presence is established. Protective personnel should quickly learn to recognize all employees and regular visitors calling on the dignitary.

(a) Advance lists should be obtained when a group of visitors is expected. Arrangements should be made with a

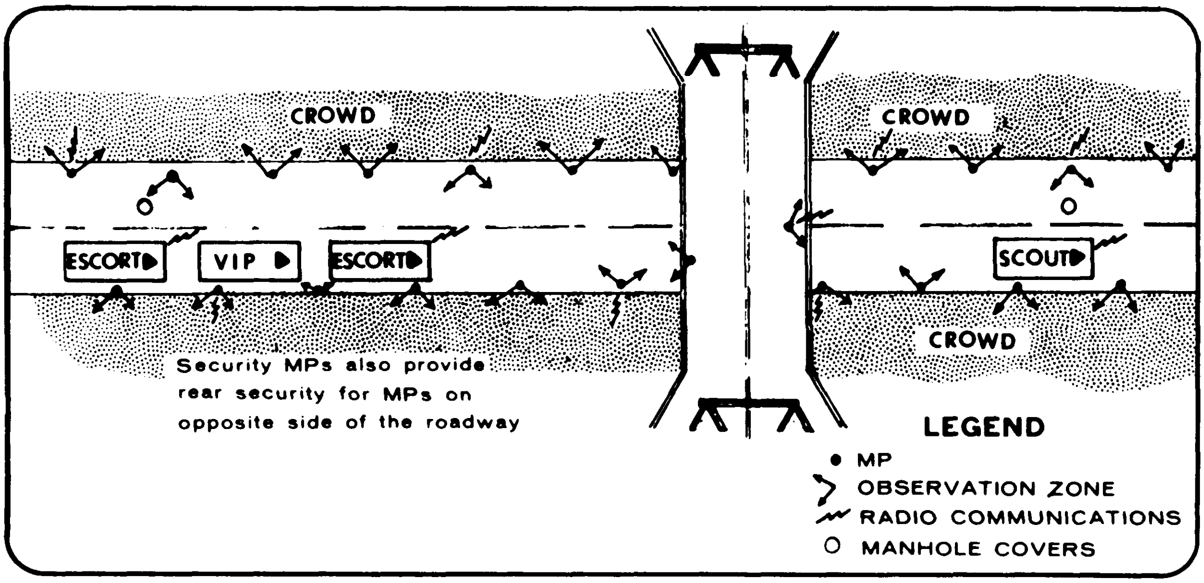


Figure 84—Sample MP placement and observation zones for convoy route security. Air cover with radio communications is recommended when appropriate.

member of the official party to identify and vouch for any unrecognized visitor.

(b) Visitors should be admitted only at specified entrances and control should be maintained to insure that they proceed directly to their approved destinations. Members of the security detail must be especially tactful and diplomatic in performing this function to avoid offending some unrecognized dignitary.

(4) Military police are stationed so that they can observe everyone and everything in the immediate vicinity of the protected person. For example, if the dignitary is in an automobile convoy and military police are lining sections of the route, a few MPs will be designated to face in the direction of the dignitary, but the majority will face the crowd so they can observe any suspicious movement (figure 84). They investigate unusual or suspicious actions tactfully and promptly. MPs place themselves between the protected person and any individual acting suspiciously. They precede the protected person into buildings, crowded areas, or dangerous places. They also flank and follow him.

(5) Bodyguards must exercise constant vigilance over the protected person; remain at all times a very short distance from him; and afford him constant protection. Bodyguards should always be armed, be experts in the use of weapons, first aid measures, know the fundamentals of judo, be well briefed as to the itinerary of the person being protected, and well rehearsed in responding to emergencies.

(6) The security detail should not enter into conversation between the protected person and other individuals. Information should be given only when solicited. All dealings with the protected person and his associates should be on a formal basis. Security detail personnel should never become involved with providing personal services for dignitaries or members of their parties. Attempts to ingratiate themselves only serve to degrade the security mission and result in an undesirable relationship. If the protected person or members of his party are friendly in their approach to the

153-846 O - 94 - 11

security detail, security personnel should react accordingly. However, the intimacy of the relationship should be established by the MP officer in charge. In the absence of guidance from him, an impersonal, business-like approach to personal contact should be the rule.

b. Use of Weapons. There is always the danger of accidental discharge and injury of innocent persons when weapons are carried. All protective personnel must be qualified to fire the weapons with which they are armed. The numbers and types of weapons earned should be appropriate to the situation and any indicated threat based on intelligence reports on the situation and the mission. In a security mission, the weapons should be ready for use.

(1) MPs in close contact with the protected person should carry a holstered sidearm of at least .38 caliber. Automatic pistols should contain a fully loaded magazine with a round in the chamber and the safety on.

(2) In areas where attackers may fire from a distance, the rifle is valuable. When attacks are made in force by armed mobs, the machinegun can be used. The machine gun is also used when attacks are made from vehicles, and when attackers are behind shields or barricades.

(3) Riot or shotguns should be available when the attack is made in a congested area where there is danger of injuring innocent persons if long-range weapons were used. They are also effective against mobs using suicidal attacks.

(4) Use of police nightsticks and riot control agents will break up and confuse a crowd, making their movement by the protective force easier. The provisions of AR 190-28 must be thoroughly understood by all protective personnel. They must **use only that degree of force reasonably** necessary.

c. Crowd control. Protective personnel should understand the principles of crowd control. They should not show prejudice or sympathy, or become involved in any grievances expressed by the crowd.

(1) When force is necessary, protective forces should move with speed and surprise. At the first sign of disorder, all leaders should be apprehended by personnel specifically assigned such duties. The real troublemakers are usually to the rear of the crowd.

(2) Protective forces should not be fooled or deterred by mob leaders who arouse and use women and children in front ranks to shield themselves from aggressive action by protective personnel. The crowd's retreat should never be hindered; it should be moved in the direction where there is space to disperse.

d. Conduct and demeanor, use of weapons, and crowd control are just a few of the many topics which might be included in the orientation or training of personnel preparing for a security mission. The complete list of subjects depends on the experience of the protective force and the specific mission it is to perform. Necessary training should be conducted using, as applicable, FM 19-10, Military Police Operations, FM 19-15, Civil Disturbance Operations; FM 19-25, Military Police Traffic Control; FM 19-20, Law Enforcement Investigations; and USACID Pam 195-1, Protective Services.

14-6 Special Requirements

As in other phases of law enforcement, investigative functions, physical securit y, and security of designated individuals, special requirements must be adhered to. As a minimum, the following should be considered applicable:

a. Advance Party Duties. Normally, the advance party is composed of at least two accredited military police criminal investigators. They should be given written authority

defining their mission, which is to coordinate and elicit cooperation from various agencies. They should make a conscious effort to avoid giving the impression that they are usurping local authority or prerogatives. Their specific duties start upon receipt of the dignitary's itinerary. The officer in charge of the detail will indicate the advance party's responsibilities. Usually the areas involved will be located at distances too far removed for the officer in charge to make personal reconnaissance. It is essential that advance party members be fully briefed in all phases of the planned activities.

(1) Specific information that they will require include:

- Complete list of the official party and staff.
- Duration of the visit, including arrival and departure times.
- Name of officials to be contacted.
- List of buildings, billets, and areas to be visited by the dignitary.

(2) In each area, their activities follow a similar pattern. They coordinate with the local provost marshal, military intelligence, local police, FBI, and other agencies such as the office of special investigations, and office of Naval intelligence, to define security responsibilities. In each case, one of the agencies involved should have the authority and primary responsibility for coordinating the protective efforts of all personnel involved in the operations. This agency, once designated by the senior commander in the area, or by the senior civilian law enforcement agency chief, will establish a working liaison with other agencies involved. The advance party contacts all local intelligence channels for pertinent information. Necessary maps and diagrams are obtained. They survey all areas to be occupied by the dignitary for layout, potential hazard, and amount and types of protective forces needed. They conduct a detailed reconnaissance of the dignitary's mute of travel. When a provost marshal is located in the area, these surveys are conducted with representatives from his office. It is important that the advance party keep in regular contact with the officer in charge for changes in schedule and transmission of special information. The advance party briefs the officer in charge on the local situation upon his arrival, and then moves to the next area on the itinerary.

b. Area and Building Surveys. All areas to be occupied or visited by the protected person should be surveyed in advance. The procedure to be described for building inspections is complete and thorough. In many instances the dignitary is a house guest of the commanding general on a military installation, on, other occasions he may be the house guest of a high-ranking governmental official. At times he may stay in a hotel occupied by numerous other guests. Certainly, all of the inspections listed in this section are not feasible.

(1) The officer in charge and his advance party must use common sense and sound judgment in establishing the best security possible under existing circumstances. In some instances the advance party can facilitate security measures by arranging for a separate house or separate floor or wing of a hotel as a billet for the official party. Normally, billeting arrangements are included in the itinerary prior to the start of the security detail.

(2) Proper building inspection entails a thorough examination from roof to basement. Blueprints of the building should be obtained. Rooms and hallways are measured visually and compared with the dimensions indicated on the building plan to locate possible hidden passageways or alcoves. Each room is examined systematically. Walls, ceilings, and floors are mentally divided into three foot squares and each square minutely examined for cracks, evidence of recent repairs and any unnatural appearance.

(3) Suspicious areas should be explained satisfactorily by reliable operating or maintenance personnel. All furniture is

carefully examined; all doors opened and drawers removed as a check for concealed compartments. All wires leading into or leaving the various rooms are traced, and all devices connected with them identified. Heating radiators, plumbing pipes, and similar equipment is carefully examined for dummy installations. All locks and locking mechanisms are inspected. After the inspection is completed, the room or building is secured until used.

14-7 Techniques of Protection

a. Protection demands **teamwork.** Success depends upon the cooperation and assistance of others. The failure of one individual may nullify the efforts of the entire organization. All personnel should be trained for the ideal system and attempt to approach that system as closely as circumstances permit. Protective personnel must be rehearsed so well that in an emergency, despite excitement and emotion, they will instinctively act correctly. Protective personnel must be familiar with the characteristics of all phases of a protective mission to include the special techniques for protecting the dignitary when he is traveling by motor vehicle, train, air, small boat, while walking, and at public assemblies.

b. Protection While Riding in Vehicles. The selection of the type vehicle to be used should be given thought. Whereas the closed car provides greater concealment and therefore better protection for a protected person, the open vehicle, such as the army 1/4 ton truck, provides much better maneuverability and observation.

(1) All automotive equipment should be in excellent mechanical condition and should be regularly inspected for signs of tampering. Drivers should be well-trained and reliable. Vehicles must be secured at all times during the security mission. An escort vehicle should precede the protected vehicle.

(2) The security vehicle should follow the protected vehicle as closely as possible consistent with driving safety. An advance car should precede the convoy by approximately one half mile to observe hazards and report on any unusual conditions.

(3) A reserve vehicle should follow the convoy a short distance in the rear for use in emergencies. The escort, follow-up, and all security vehicles should maintain radio contact. Whenever possible, a member of the security detail is placed in the protected person's vehicle. Under extreme conditions, when greater security is necessary, one or two dummy vehicles, carrying individuals similar in appearance to the protected official, may be included in the convoy.

(4) Fixed posts at bridges, underpasses, and railroad crossings may be established when deemed necessary. An alternate route should be arranged for emergency requirements. Unless indicated otherwise by competent authority, the convoy will conform with local traffic regulations and will maintain a rate of speed consistent with road conditions.

(5) Each situation is evaluated to determine the degree of security that is practical and necessary. For example, on a military installation it is normal procedure for ranking officers to ride in the vehicle immediately behind the escorted official's vehicle. The security vehicle may drop behind and follow at a discreet distance when hazards are minimal. Good judgment on the part of the officer in charge will be necessary in solving the various situations that arise. Figure 85 shows a typical motorcade arrangement.

c. Travel by Train. Generally, the greatest potential security hazards exist at the points where the protected person boards or leaves the train. Usually, this is a congested area with numerous individuals carrying all sorts of bags, packages, and containers. In the study of assassination techniques, the large number of attempts in this type of

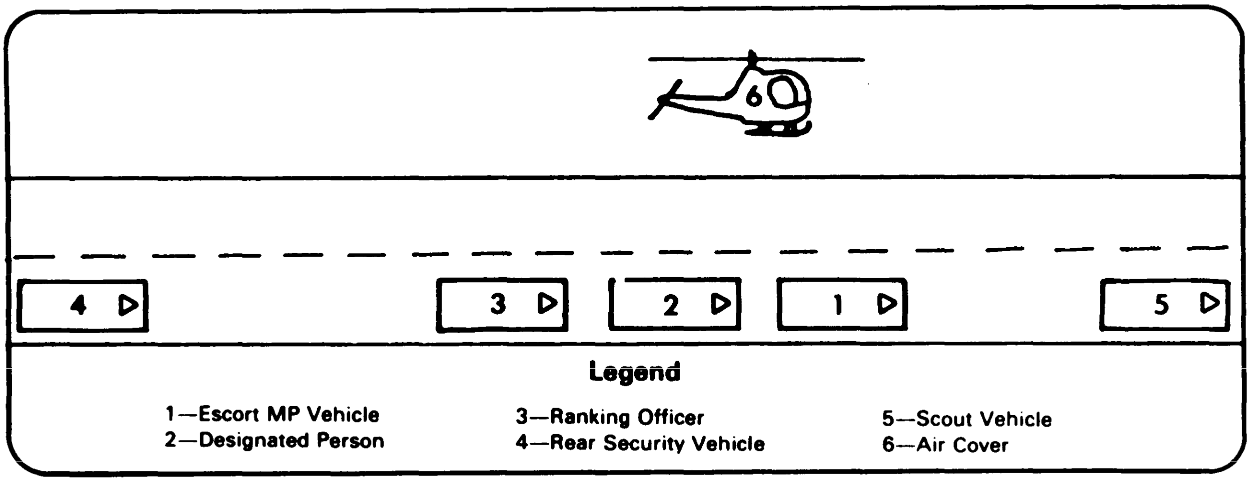


Figure 85—Motorcade arrangement.

location is noteworthy. When possible, the area should be closed to the general public or the protected person should board at an isolated siding.

When a private car is assigned the party, it should be attached to the rear of the train. The security detail should be in control of all entrances of the car. When the train is stopped they assume positions covering all avenues of approach to the car.

If the protected person leaves the train for a temporary period, constant security should be maintained on the train until the protected person returns and the train departs. Prior coordination should be made with railway officials for exact scheduling of stops en route. Railroad police and local police at scheduled stops can be contacted for standby assistance.

When deemed necessary, advance and rear guard trains may be scheduled to precede and follow the official train at safe distances, Under certain circumstances, additional security personnel may be placed in other cars of the train, seated among passengers, as an additional safeguard.

d. Travel by Air. Normally, a special plane is assigned for transporting the dignitary and his official party. Technical safety factors such as clearance of operating personnel and control in flight are responsibilities of the operating agency when performed by the military forces. The most dangerous periods, as in train movements, are boarding and departure times.

(1) All structures offering observation of the boarding area should be adequately secured either by closing off when not used or by strategic placement of a security detail. When a large crowd is expected for take-off ceremonies, barricades and large forces of uniformed military and/or civilian police should be included in the planning. The plane designated for the protected person should be kept under constant guard when not operational. All unauthorized persons should be kept away from contact with the plane.

(2) When the destination is another base, advance arrangements should be made with the local provost marshal for additional security and transportation requirements as needed. Sufficient transportation is normally scheduled for the protected person and his party. It should not be forgotten, however, that arrangements must be made for accompanying security personnel.

e. Travel by Small Watercraft. When planning for a cruise, the boats selected should be of a type and size capable of withstanding weather and surf conditions that may be encountered. A thorough inspec tion of the boat designated for the protected

person should be made with responsible ship personnel. The inspection is primarily for unauthorized persons stowing away and for any suspicious objects or packages. An additional check should be made for adequate lifesaving and emergency facilities. Security personnel should be alert for other craft approaching the protected person's boat. Arrangements should be made for boats to precede and follow the protected boat.

f. Protection While Walking. One of the best protective measures is varying the selection of walking times and routes. The security detail accompanying the protected person should be positioned to cover all avenues of access. Additional security personnel should be available in the area. A security vehicle should cruise in the immediaiate vicinity. Local police agencies can be of special value in adding background security in these instances.

g. Protection at Public Assemblies. A careful search and inspection of the area should be made at the time protection is established. A physical defense zone should be set up immediately around the protected person and additional concentric defense areas should be added to the greatest possible extent. Protection in the defense zone is provided by protective personnel, permanent or temporary type barricades, and a combination of the above two resources. Screening points should be established to admit passage of authorized persons and materials. Observant and inconspicuous security personnel should patrol among the crowd. Maximum use should be made of security aids such as flood and spotlights, communications, emergency equipment, special weapons, locks, barricaded areas, and bulletproof equipment and materials.

h. Protection While in a Residence. The protective detail should occupy at least one protective ring. At least two additional areas should be established on the outer perimeter. There must be a pass system for the staff and frequent visitors. Food suppliers should be checked and food selection and handling should be controlled. Mail and packages should be fluoroscope. Periodic inspections should be made of premises for safety hazards, lethal devices, and sufficiency of security equipment. Adequate communications should be maintained. All possible emergency situations should be considered. Persons providing personal or domestic services for the dignitary and his party should be screened in advance and should receive a security briefing prior to the dignitary's arrival. Accomplishing this task is the responsibility of the advanced party.

14-8 Critique And After Action Report

a. The **critique** is the final stage of the security mission. It is conducted so that all participants will have a clear, orderly idea of what was done properly and what was done improperly. To improve operations, intelligent, tactful, and constructive criticism is necessary. The critique can be most effective if held as soon as practicable after the mission is completed.

(1) The critique is so important that it must be considered a phase of the security mission itself. The effectiveness of this phase depends upon the flexibility with which the officer in charge employs it. In conducting the critique, the officer in charge must not be sarcastic; he must make criticism or comments in a straightforward, impersonal manner. He should criticize individuals in private; praise them in public. Participants should leave the critique with a favorable attitude toward the security mission and a desire to improve the next one. Examples of personal initiative or ingenuity, type of errors, and ways for correcting them should be covered specifically. Protective personnel should be encouraged to participate in the controlled discussion. They feel then that the critique is a period for learning rather

than a time set aside for criticism of their performance.

(2) Steps in conducting the critique. The critique cannot be planned as thoroughly as other phases of the mission, because the points to be covered are influenced directly by the performance of protective personnel. Advance planning can include the time and place of the critique, and the general outline to be followed. During other stages the officer in charge and supervisors can take notes to guide the critique, but detailed planning is not practical. However, the officer in charge can insure complete coverage of the important elements by following this general procedure:

(a) Restate objective of the mission— This will enable participants to start on a common ground. This is necessary because the participants who were concerned with a particular aspect of the subject may have forgotten the overall objective.

(b) Review procedures and techniques employed— In this step briefly summarize the methods used to attain the objective.

(c) Evaluate performance—This is the most important part of the critique. Using notes taken during the mission, the officer in charge points out and discusses the strong points. Then he brings out the weaker points and makes suggestions for improvement. He must be careful not to talk down to the group. All remarks must be specific and impersonal. Personnel will not profit from generalities.

(d) Control the group in discussion— The officer in charge will discuss the points he has mentioned and suggest other points for discussion.

(e) Summarize— The critique is concluded with a brief but comprehensive summation of the points brought out. The officer in charge can suggest study and practice to overcome deficiencies. The critique is business-like. It must not degenerate into a lecture.

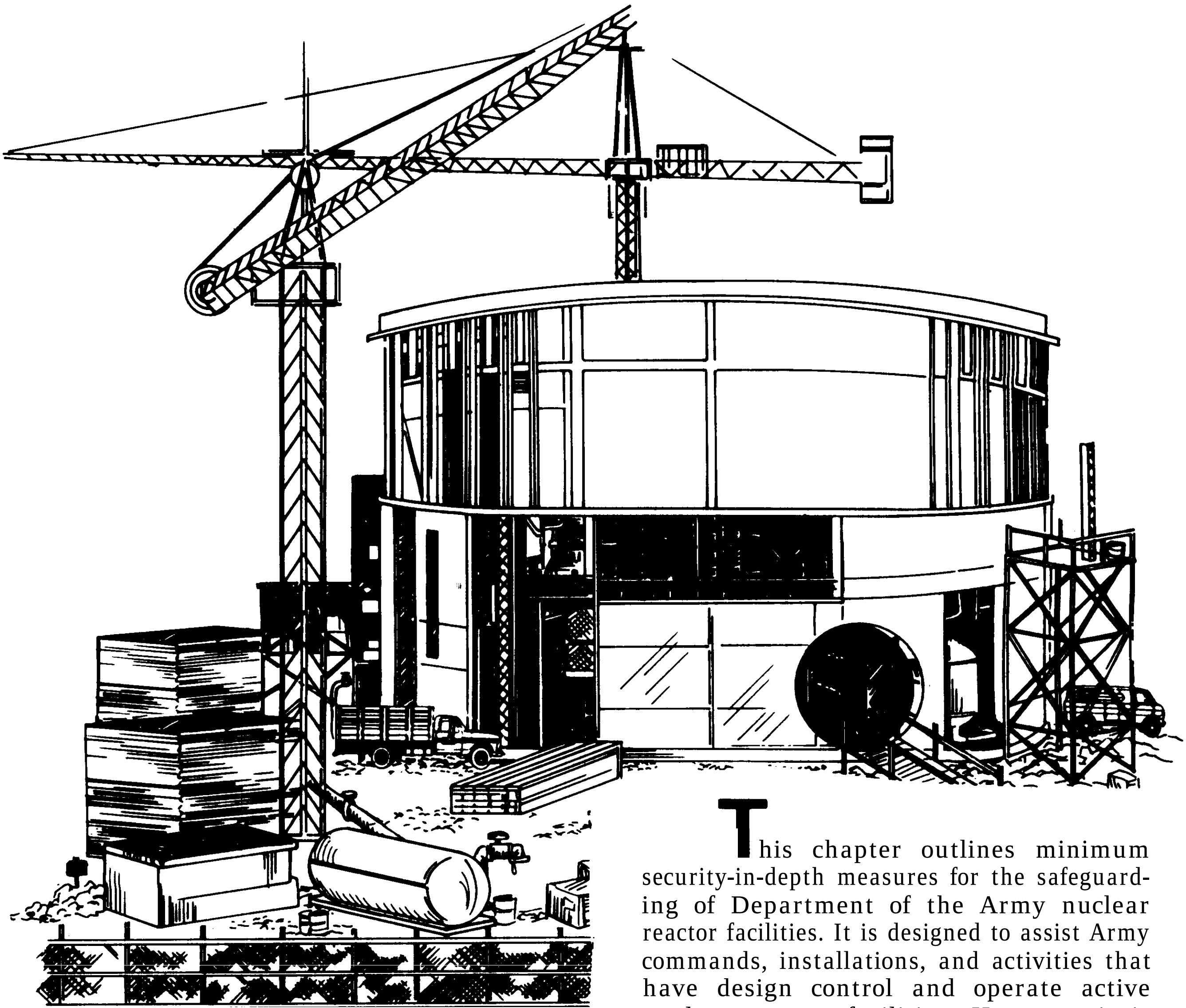
b. The **after-action report** is a resume—highlights of the security mission, written in narrative style. It is written as soon after completion of the mission as practicable.

(1) Notes taken by supervisory personnel during the operations will serve as a basis for compiling this report. Emphasis is placed upon the difficulties encountered and the procedures necessary to eliminate them.

(2) Recommendations for improvement, especially in planning, coordination, personnel and equipment, are written in detail. A file copy is retained for use in improving future operations.

Chapter 15

Nuclear Reactor Facilities



This chapter outlines minimum security-in-depth measures for the safeguarding of Department of the Army nuclear reactor facilities. It is designed to assist Army commands, installations, and activities that have design control and operate active nuclear reactor facilities. However, it is recognized that because of physical plant differences, not all requirements will apply.

15-1 Security Engineering

Security engineering begins with the selection of a site. It entails a security assessment of the construction blueprints and considers the following:

- Site isolation
- Access routes
- Security force location and response time
- Landscape
- Terrain characteristics
- Climate.

15-2 Responsibilities

a. Security **standards and measures** for US Army reactor facilities are provided by the Deputy Chief of Staff for Personnel. Supervision, guidance, and support for the protection of Army nuclear reactor facilities is provided by the responsible command and installation staffs. AR 385-80 outlines other Army staff agency responsibilities in protection of US Army nuclear reactor facilities.

b. The **reactor commander** must comply with all applicable physical security standards, measures, and procedures (ARs, DNA, DOD, NRC, etc.). He must develop and maintain a comprehensive security plan (chapter 3, AR 50-5).

15-3 Security Components For a Reactor Facility

- Guard forces (chapter 9).
- Access controls (chapter 4).
- Explosive and metal detectors (appendix D).
- Identification systems (chapter 4).
- Intrusion detection devices (chapter 7).
- Closed circuit television surveillance systems (appendix M).
- Computerized microwave system hardware and software.

15-4 Prevention and Protection

a. Protect nuclear reactor facilities from all forms of sabotage, espionage, and overt attacks.

b. Prevent theft or diversion of special nuclear material.

c. Prevent unauthorized access and damage to nuclear reactor facilities.

15-5 Essential Requirements

a. Restricted areas criteria.

☐ AR 380-20, Restricted Areas, establishes that exclusion/vital areas must be surrounded by structural barriers and have appropriate signs posted. (See chapter 4, also).

☐ Areas contain:

- Special nuclear material (SNM).
- Nuclear reactor(s).
- Control consoles.

☐ Contained within a limited area also surrounded by at least an additional structural barrier (see chapter 5, Protective Barriers).

b. Special **nuclear material storage areas.**

(1) If not installed in the reactor assembly, construction of walls, roof, and floor will be of one of the following

- Steel at least 1½-inches thick.
- Nonreinforced concrete at least 12 inches thick.

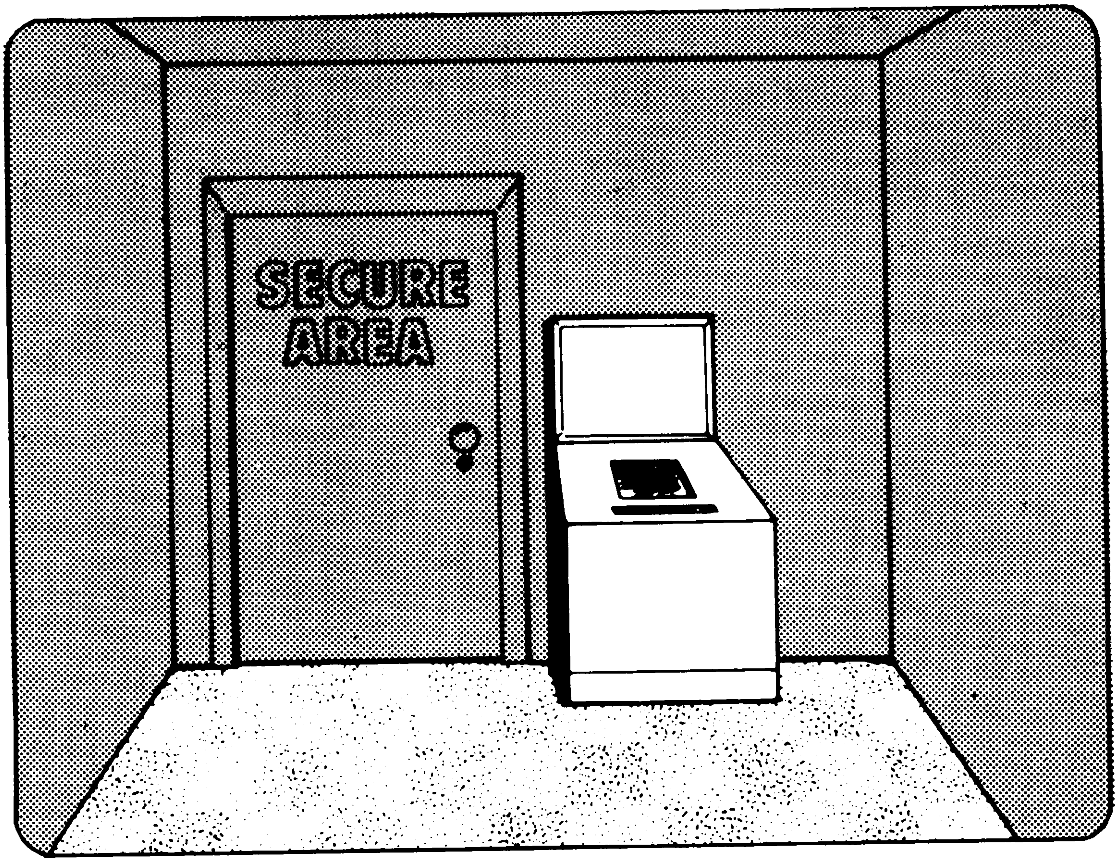


Figure 86—Palm print readers help control access.

(2) Access doors must meet these guidelines:

- ☐ Kept to a minimum.
- ☐ Constructed of steel at least 1 inch thick.
- ☐ Exclusive of the locking mechanism.
- ☐ Secured with at least 2 locking devices.
- ☐ Locks must consist of a three-position, manipulation-resistant, dial-type, built-in combination and any one high-security padlock with high-security hasps.

c. Entry control must be formalized and maintained. It must insure positive identification prior to admission and restrict access to limited and exclusion areas.

(1) Access control procedures and equipment are different from host installation badges (section XI, AR 606-5, and chapter 4 of this manual).

(2) Formal entry control rosters must be maintained.

(3) A visitor control system must be established. The system should be periodically reviewed to determine who visits the facility most and when.

(4) Package, material and vehicle control must include:

- A positive system.
- Prevention of unauthorized removal of SNM—a necessity.
- Any sealed package requires a signed

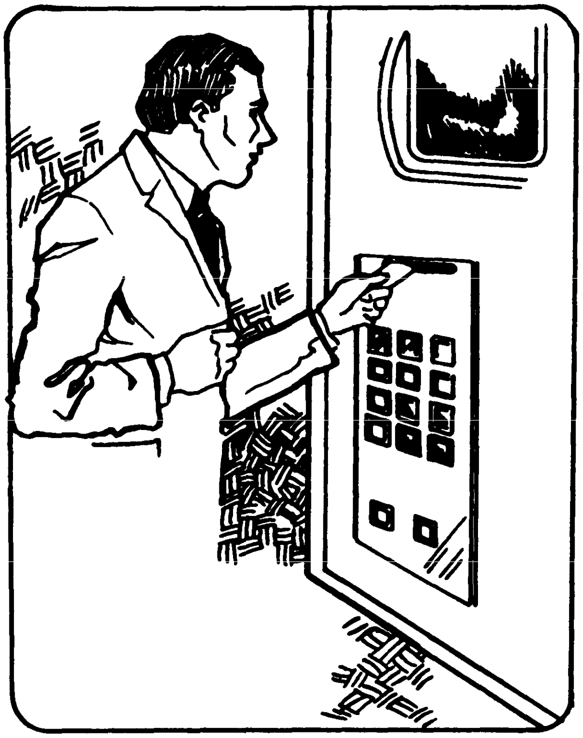


Figure 87—Electric card reader.

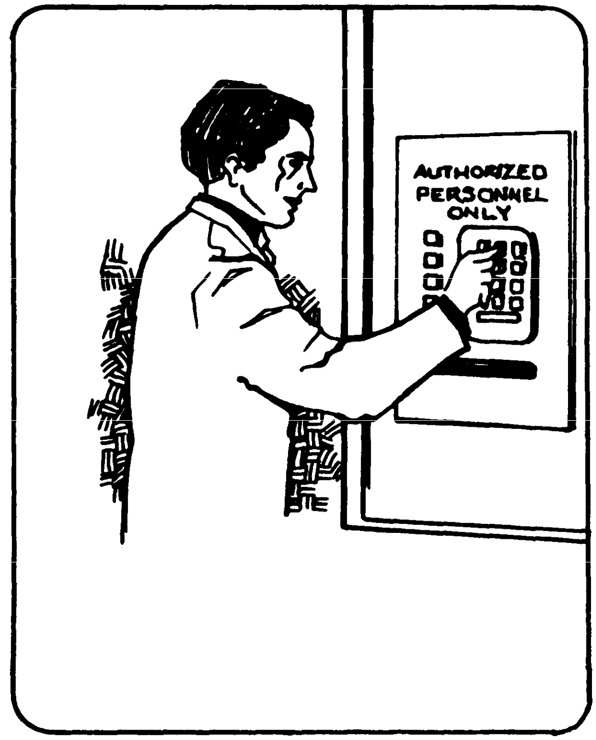


Figure 88—Example of digital code access control equipment.

DA Form 1818, Individual Property Pass. **Authority to sign DA Form 1818** must be designated in writing. Reactor commanders may designate other items to be controlled by DA Form 1818.

- Other packages and material must be examined for unauthorized items.

(5) Vehicle entry to restricted area must be limited to mission-essential vehicles only.

(6) Types of equipment suitable for access control to a nuclear reactor facility.

- ❑ Palm print readers (figure 88)
- ❑ Signature identification devices
- ❑ Electric card readers (figure 87)
- ❑ Fingerprint readers
- ❑ Voiceprint identification
- ❑ Digital code access control.

15-6 Intrusion Detection Systems

These systems were discussed at length in chapter 7. At this point we'll list their special application at nuclear facilities.

- ■ Used in unoccupied nuclear reactor facility exclusion/vital areas.
- ■ All alarms must sound in at least one continuously manned station.
- ■ Station does not need to be located onsite.
- ■ Alarm sounding must indicate where the alarm was caused and vital areas identified accordingly.



Figure 89—Sample IDS application at a nuclear facility.

■ Alarms must be:

- Self-checking king.
- Tamper-indicating.
- Functionally tested for operability and required performance at the beginning and end of each interval during which they are used.
- Tested not less frequently than once every 24 hours.

■ Alarm annunciator panel (monitor) location must be identified and secured.

■ Record must be maintained of each alarm (nuisance alarm, alarm check/test, tamper indication). The record must show the following information:

□ Identify type of alarm
□ Alarm location
□ Alarm circuit
□ Date and time of activation
□ Details of response by security guards.

15-7 Lock and Control Key Control

a. Each SNM storage structure entrance must be secured with at least two locking devices.

b. Other entrance doors or gates to the facility must be secured with a locking device that provides protection equal to MILSPEC 17802.

c. Custodian of keys and locks to buildings or ar33eas containing SNM must be designated

by the reactor commander, in writing. Keys must be available only to authorized individuals.

d. Key registers must be maintained.

e. During nonworking hours depositories must be available where keys are secured. Keys must not be removed from the facility and no **one** individual will have access to both keys and/or combinations of a structure containing SNM.

f. At the end of each operational shift or period, inventories must be made concerning key registers, key boards, and key depositories. Inventories must remain on file at least 60 days. In case of incidents involving investigations, they must be maintained on file until the investigation is terminated.

g. Six-month requirements:

- Key padlock rotation.
- Combinations on combination locks must be changed immediately upon compromise, transfer, or loss of individual with knowledge of combination.
- Records of the 6-month requirements must remain on file for 1 year.

15-8 Custodian and Inventories

- A primary and alternate custodian must be designated in writing, concerning responsibility and accountability.
- The primary custodian or his alternate must conduct weekly inventories.
- Irregularity must be immediately reported to the proper authority.
- A joint monthly inventory must be conducted by the custodian and a disinterested person.
- Inventories must reflect the following:
  - Serial numbers
  - Quantity
  - Weight
  - Be recorded and authenticated.

15-9 SNM Hazard/ Inaccessibility

- If radioactive and it presents a health hazard, SNM item must be inaccessible.
- A joint inventory must be conducted by custodian and a disinterested person.
- Railway type seal (or equivalent) must be used and affixed through the high-security hasp.
- All seal serial numbers must be recorded.
- Excess seals must have the same degree of security as keys and high security locks and hasps.
- Seals must be inspected daily by custodian or alternate.
- Seal inspection results remain on file for at least 60 days, or longer, in case of an investigation.

15-10 Communications

a. Each individual controlling access into limited, exclusion or vital areas must maintain positive communications with an individual at a continuously manned location. The individual at the continuously manned location will call for assistance from other guards or the response force, if necessary.

b. As a minimum, one two-way voice radio communication link will be established in addition to conventional telephone service between security posts and supporting security agencies.

c. All communications equipment must be capable of remaining operable from independent power sources in the event of loss of primary power. Such independent power sources may be provided through standby generators or batteries.

d. Communications equipment will be tested for operability y and performance not less than once at the beginning of each workshift.

e. Positive procedures must be developed to provide notice when a limited or exclusion area is in a state of duress.

15-11 Protective Lighting

Security lighting must be provided to discourage unauthorized entry and to facilitate detection of intruders approaching or attempting to gain entry into the facilities. Perimeter and access control point lighting will be positioned to prevent blinding of sentries from glare and to avoid silhouetting or highlighting of sentries. Such lighting must be controlled by the securit y force. (See chapter 6 for specifics on protective lighting.)

15-12 Security Force

a. Commanders will plan for an armed force of sufficient strength and composition to insure enforcement of established security measures and to detect unauthorized presence or activity of persons within the limited or exclusion area on a 24-hour basis.

b. Commanders must develop emergency procedures to cope with any unauthorized presence and/or activity in the limited exclusion/vital areas. As a minimum, a 15-man response force must be able to reach a security problem within 5 minutes of verified discovery. In the case of an unverified problem, the 5 minutes begin when two or three members of the force verify the problem and call for the remainder of the force. Security and response force personnel will use the force necessary to prevent any unauthorized attempts to remove special nuclear material from the facility. Commanders must make provisions for any additional response forces that may be required during times of emergency. These contingency provisions must be included as an annex to the physical security plan. Plans should be kept current and, as a minimum, tested semiannually.

c. Security and response forces should be armed with a mix of weapons suitable to the environment in which they will be employed.

15-13 Survey and Plan

A physical security survey should be conducted by qualified physical security specialists of each facility. DA Form 2806, Physical Security Survey, should be used and copies of the survey, including reports of corrective action if required, forwarded through command channels to HQDA (DAPE-HRE), WASH DC 20310 (AR 190-13).

A physical security plan should be prepared for each nuclear reactor facility and be integrated with the plans of host military installations. Guidance and format for the physical security plan are contained in appendix F. Detailed specifications, photographs, drawings, guard orders, and sketch maps, as appropriate, should be included as annexes. Plans should be reviewed and approved at major command level.

15-14 Shipment Security

a. Intra-installation transportation security is a command responsibility, and procedures should be developed accordingly.

b. All transfers of special nuclear material between security areas should be escorted by at least two people, one of whom is armed. Escorts should have radio communications capability, as appropriate.

c. Personnel must be trained in civil disturbance formations and small unit tactics (FM 19-15 and TC 7-1).

d. Security is governed by:

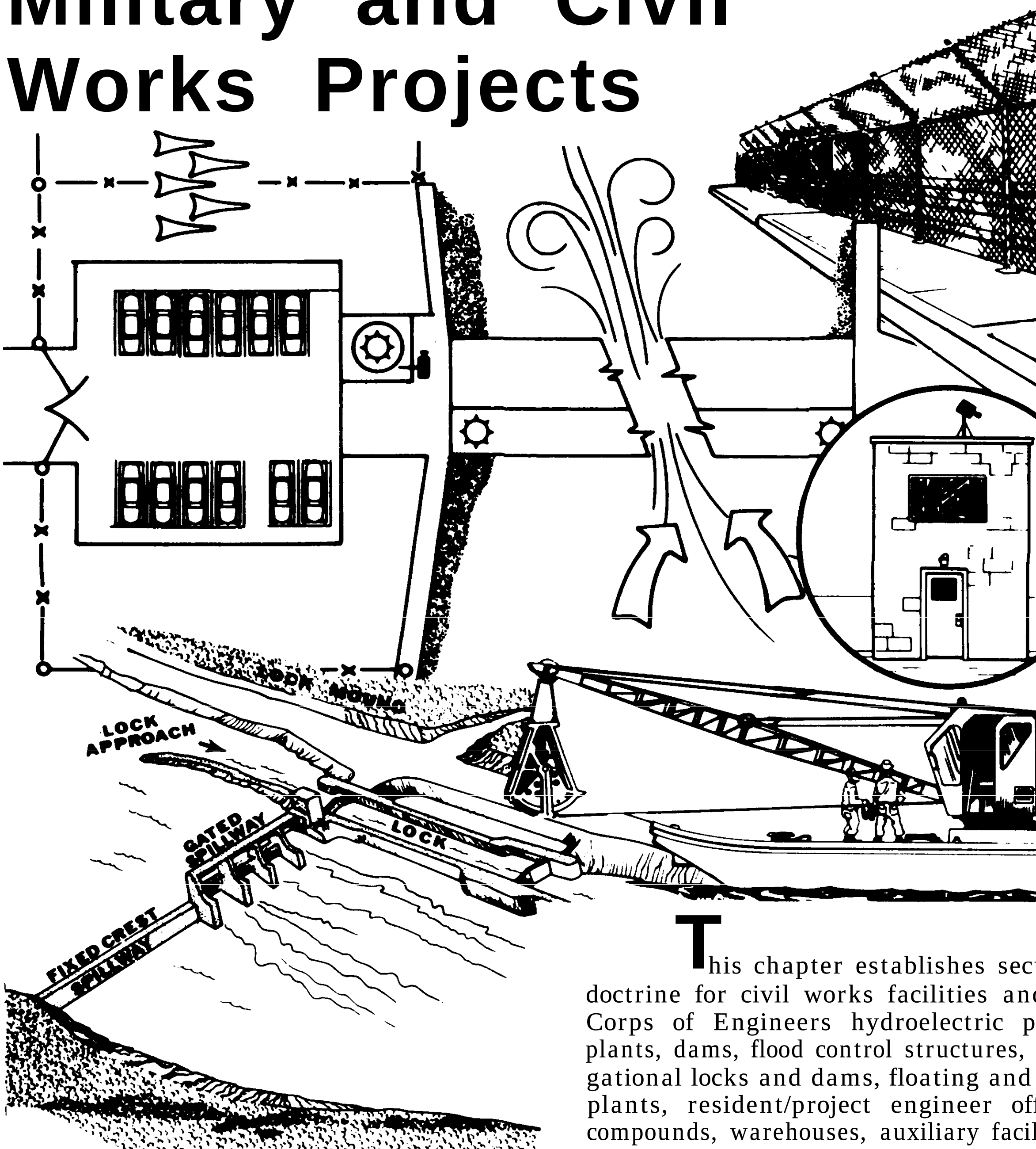
- AR 55-355, and Department of Transportation, Title 49, Code of Federal Regulations (CFR) when commercial camera are used.
- Nuclear Regulatory Commission (NRC), Title 10, Part 73, CFR, when SNM is transported in coordination with the NRC or when Department of Energy courier service is used.

15-15 Definitions

See appendix S.

Chapter 16

Military and Civil Works Projects



This chapter establishes security doctrine for civil works facilities and for Corps of Engineers hydroelectric power plants, dams, flood control structures, navigational locks and dams, floating and land plants, resident/project engineer offices, compounds, warehouses, auxiliary facilities, projects, and construction sites.

Physical security planning for Corps of Engineers projects should be based on a total integrated systems approach and should include, as a minimum, the following factors:

- ■ Environmental and human aspects of the project to include criminal, political, and economic considerations, accessibility, and locality.
- ■ Importance of the projector activity to the national defense, OCE using agency, and environment.
- ■ Vulnerability of the project to loss, theft, pilferage, or willful damage of equipment or supplies.
- ■ Operational requirements to include aesthetics and access to the public.

16-1 Applicability

Guidance contained in this chapter applies to all Corps of Engineers divisions, districts, and field operating agencies.

16-2 Basic Philosophy

The basic philosophy of the Corps of Engineers encourages maximum use of projects for educational and recreational purposes. However, access to project facilities considered vulnerable/critical as defined in this chapter should be restricted or denied.

16-3 Security Aspects

a. In providing security to projects, district engineers should use well designed, quality perimeter fencing (OCE Drawing 40-16-08) which, where feasible, is lighted during hours of darkness to deny or discourage access to critical facilities or areas. Perimeter security fencing must be standard Corps of Engineers design or an aesthetic design equally secure and be set back sufficiently from the facility to prevent damage from explosives or flammable material thrown into the area. Where not practical to erect barrier fencing, ground level windows should be covered by heavy gauge security screen or equivalent aesthetic designed security material.

b. Also necessary are systems for vehicle and personnel control, adequate communications (secure inhouse telephone systems), effective liaison with responsible law enforcement agencies, and a security awareness program for all Corps personnel.

c. Permanent hire personnel deemed by the district engineer as being in a noncritical/sensitive position, should undergo limited and/or extended NACI checks.

d. All personnel should be trained thoroughly prior to assumption of duties and responsibilities. Training should be designed to accommodate formalized training (classroom), informal training (on-the-job), and ongoing training. Passing criteria, evaluation

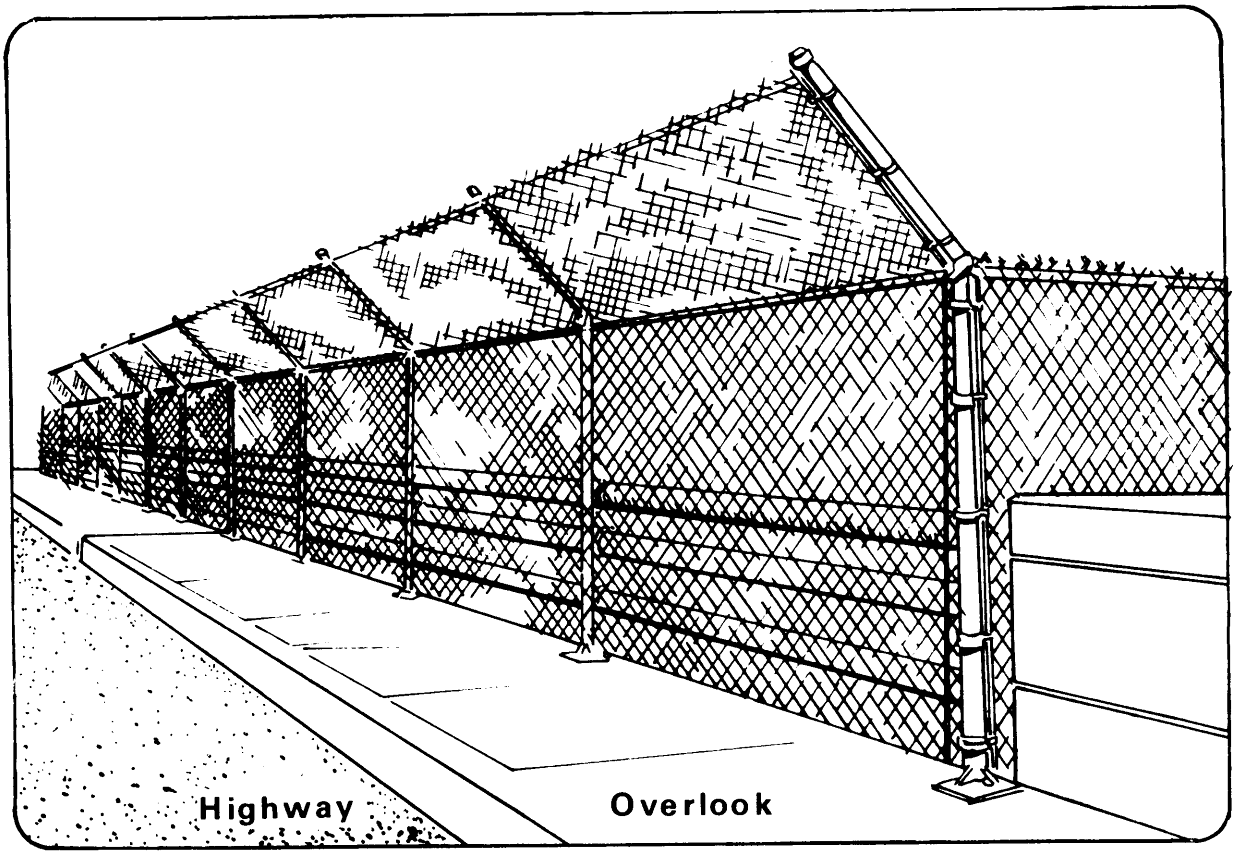


Figure 91—Typical protective fence for dam with highway.

and efficiency ratings should be used to the maximum. Where contract guards are employed, specific levels of proficiency expected should be identified in the contract specification (appendix G).

e. Discussion and/or communications concerning project security measures should be safeguarded. Written communication should be designated "FOR OFFICIAL USE ONLY," and discussion restricted to persons with a need to know. Appropriate secure communications procedures should be used in all transmissions.

f. Because of varying conditions relating to the location of civil works projects, it may be necessary to develop special security requirements for certain projects. For example, a dam that has a state or Federal highway across the top, transformers, and/or switch yards, may be protected by fencing as shown in figure 91. The primary objective should be to maintain a controlled security posture. Generally, this posture can be attained by imposing reasonable restrictions of free access to critical areas of a project. When establishing the degree of protection necessary, security requirements should be coordinated with the district security officer, who, in turn, should coordinate with local law enforcement agencies in establishing a threat analysis.

Hydroelectric Power Plants

Section II

Hydroelectric power plants are generally the primary feature of a multipurpose project. They are designed, constructed and operated by the US Army Corps of Engineers with civil funding appropriated by Congress and are located throughout the United States. These facilities are used for:

- ❑ Flood control
- ❑ Electric power production
- ❑ Public recreation
- ❑ Fishing
- ❑ Boating
- ❑ Land conservation
- ❑ Forestry.

16-4 Critical/Sensitive Functional Areas

The following areas demand security attention:

- ❑ Powerhouses
- ❑ Switchyards
- ❑ Intake/outlet structures
- ❑ Transformers
- ❑ Generators.

16-5 Public Access

a. The general public should be given access to only the visitor's lobby, display areas, overlook facilities, and restrooms associated therewith, unless on a conducted tour under the direct supervision of Corps personnel. During high visitation periods, trained temporary hire guides may be used to greet the public and conduct supervised tours. Controlled visitation should prevail at all times.

b. Packages, briefcases, camera and gadget bags, suitcases, etc., must not be permitted in any area of the powerhouse.

c. Explosive material should not be allowed within or near the powerhouse or switch yards. Firearms should also be prohibited except when carried by authorized Corps personnel or persons in the law enforcement community. During the winter season, on weekends, holidays, and at other times when public visitor activities cannot be monitored, powerhouse entrances and parking area gates should be kept locked.

16-6 Security Measures

- Fence/barriers (chapter 5).
- Protective lighting (chapter 6).
- Intrusion detectors and sensors (chapter 7).
- Metal and explosive detectors (appendix D).
- Access control and identification systems (chapter 4).
- Closed circuit television surveillance (appendix M).
- Lock and key control (chapter 8).
- Security force (chapter 9).
- Contingency forces (chapter 9).
- Contractor personnel (appendix G).

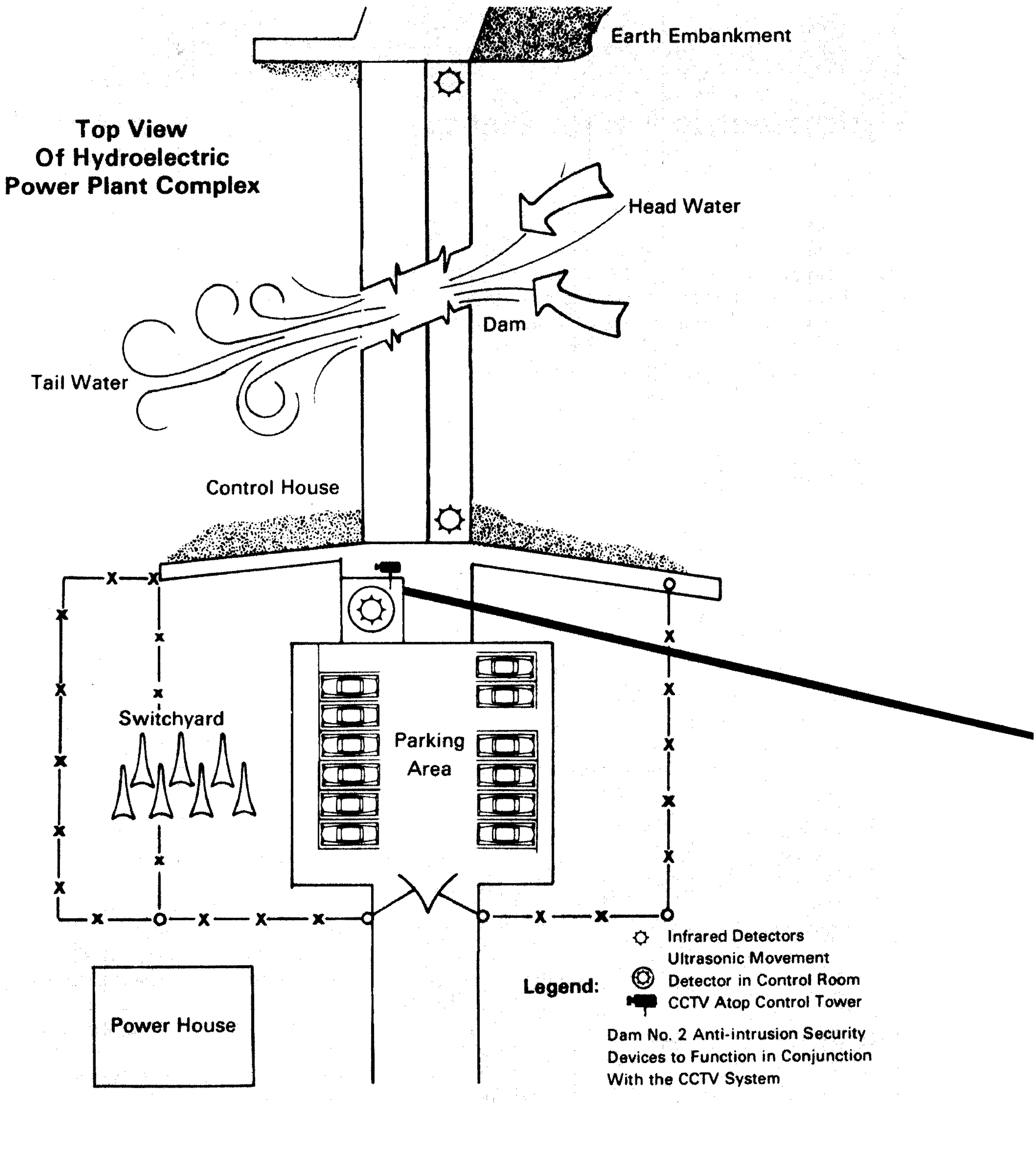


Figure 92—Sample security setup for dam, including CCTV.

16-7 Intrusion Detection Devices

These devices are especially ideal for remote facilities or land areas adjacent to dam structures. Detailed explanation is contained in specific Corps of Engineers regulations and chapter 7 of this manual.

16-8 Closed Circuit Television

In an effort to monitor personnel activity, the use of CCTV (figure 92) will greatly improve security and public safety, especially for remote facilities such as the following (see appendix M):

- ❑ Switchyards
- ❑ Transformers
- ❑ Head and tail water
- ❑ Powerhouse compounds.

16-9 Guard Forces

During maximum security condition, security officers should identify areas for guard forces, to include static, mobile, and response force protection.

Dams

Section III

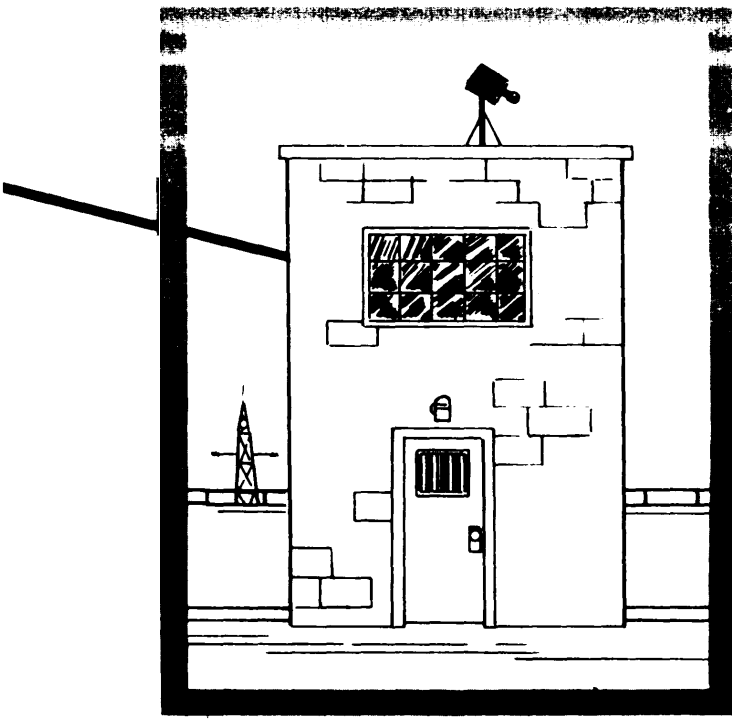


Figure 93-Detail of control structure.

16-10 Control Structures

Flood control dams provide flood control as well as water supply, public recreation, fishing, boating, land and forestry conservation.

a. The control structure, generally a concrete tower-type building at the dam site, houses the inlet and outlet control gates and is the critical facility at such projects (figure 93). Project visitation is encouraged; however, public access to control mechanisms should be denied or restrained. Increased physical security measures should be taken to safeguard all facilities housing control mechanisms.

b. Since intake valves are critical to the operation of the entire dam structures, the following special security measures should be considered:

(1) Use of personnel surveillance/CCTV to detect floating or drifting high explosives into the dam's intake valves.

(2) Use of buoy lines or log booms strategically placed in front of intake valves to prevent access.

16-11 Protective Lighting

Protective lighting should be used to illuminate critical control structures and be of sufficient brightness for observation of critical areas such as intake and outlet structures. Transformer decks, generators, switchyards, exterior powerhouse doors/gates should be considered in developing any protective lighting plan.

Navigational Locks and Dams — Section IV

Navigational locks and dams (figure 94) are the primary features of US inland navigational systems located throughout the United States and its possessions. These facilities provide an economical means of water transportation which is critical to the national economy.

16-12 Public Access

a. Public visitation and use are encouraged; however, visitor facilities should be developed only where warranted.

b. The public should not be allowed access to lock walls, lock and tainter gates, control rooms, operating machinery, or the power supply unless under supervision of Corps personnel.

c. All entrance doors to control houses and control shelters for all locks should be kept securely locked at all times.

d. During supevised tours, no packages, briefcases, or suitcases will be permitted in critical areas.

16-13 Security Safety

Access to the lock wall should be secured by fencing (Corps of Engineers Standard Drawing 40-16-08, Type FE-6). Also, at least a 20-foot clear zone should be established.

16-14 Protective Lighting

The following guidelines apply to the use of protective lighting at lock and dam facilities:

Inside and outside chambers.
- Upper and lower gate and controls.
- Dam gate spillway component security.
- Restricted access to system controls.
- Walkways and gate hoists.
- Restricted access to hydraulic structures.

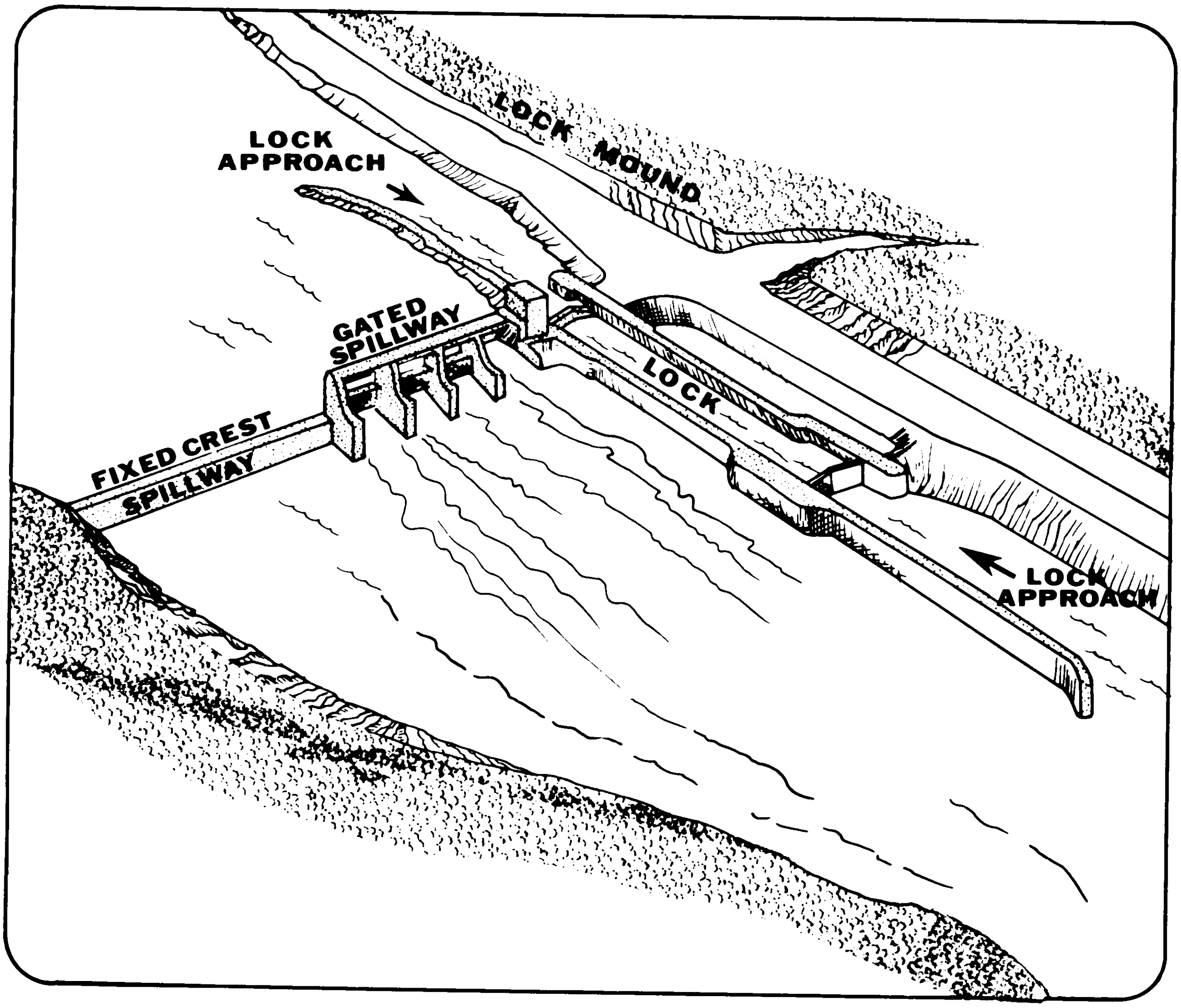


Figure 94—Typical navigational lock and dam.

16-15 Inside/Outside Chambers

- Periodic inspection of walls.
- Identify and protect or restrict access to structural areas that could conceal high explosive charges.
- Barriers should be erected to eliminate foot traffic by public and access to tunnels and pumps.
- Periodic inspection of upper and lower gate structures for high explosive charges and for objects that, if pinned in the gates, would cause severe damage to gate structures and supporting hydraulic pumps.
- Consider use of CCTV for visual surveillance of the entire project from control building.

Floating and Land Plants

Section V

Land and floating plants (figure 95) support intercostal river navigational systems and ocean ports throughout the United States and its possessions.

16-16 Floating Plants

a. Corps of Engineers floating plants include:

(1) Dredges.

(2) Barges.

(3) Tug, tow, snag, derrick and survey boats.

(4) Work and patrol boats.

b. Floating plant security measures:

(1) Establish a physical security plan for boat operations, drydock or waterborne service.

(2) Notify civil authorities/Coast Guard in case of emergencies.

(3) Continual surveillance of area– during operation, rest breaks, and after termination of workday.

c. Vessel damage/larceny prevention measures:

(1) Brief personnel on the need for security.

(2) Establish port watch for off-duty periods.

(3) Use transom locks to secure boat motors.

(4) Sleep on board vessels when appropriate.

(5) Remove small boats from the water whenever feasible and place in secure areas. Use of rented marina facilities is encouraged.

d. Security considerations should include the following:

(1) Sea cocks and valves should be secured to prevent sinking of vessel.

(2) Electric power source, to include controls, should have security measures applied to restrict access and/or tampering.

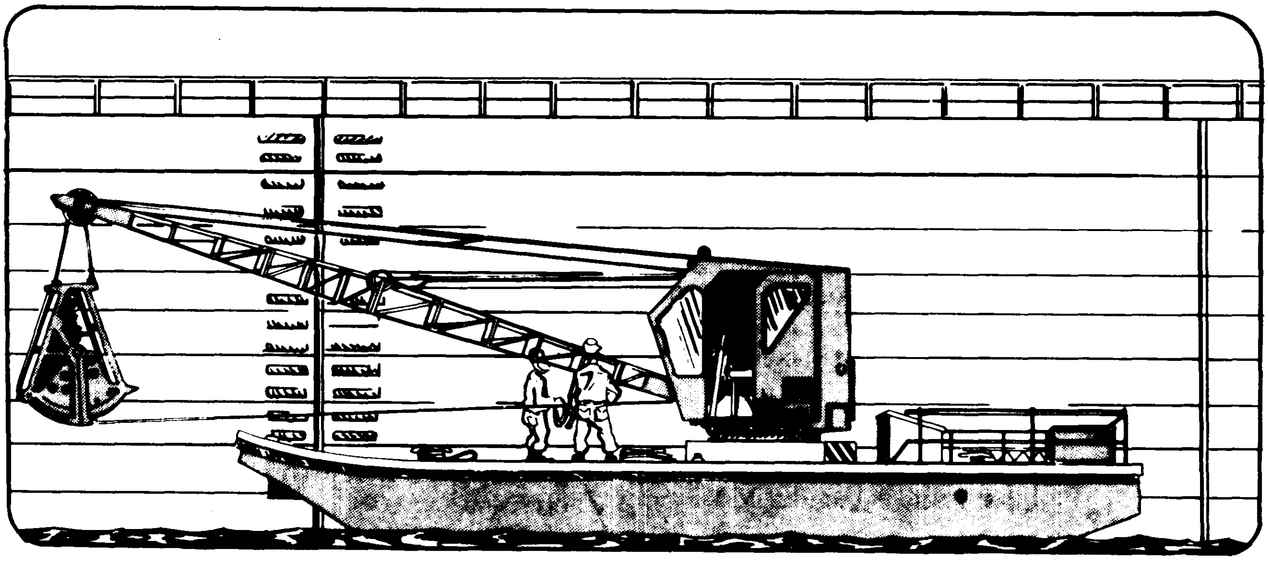


Figure 95—A dredge is one example of a floating plant.

(3) Ground fuel storage tanks and tanks located on vessels should have locking caps and protective lighting.

16-17 Land Plants

a. Corps of Engineers land plants include:

- ❑ Ports.
- ❑ Shipyards and machine shops.
- ❑ Harbors.
- ❑ Marine terminals.
- ❑ Docks and piers.
- ❑ Lighthouses.
- ❑ Maintenance yards, construction yards, and warehouses.

b. Land plant security measures. Standard Corps of Engineers compound perimeter security fences and gates (Standard Drawing 40-16-08, Type FE-6) with clear zones, be secured with a 3-foot-8-inch case hardened steel chain with case hardened padlocks.

c. Protective lighting— see chapter 6.

d. Building lock and key control systems.

(1) All exterior doors and high value storage areas should be secured with series 1000 (86), mortise, dead bolt Iockset with a 1-inch throw or a case hardened steel hasp and padlock and be rotated annually.

(2) See chapter 8.

(3) All exposed bolts should be protected by a baffle plate (strip of metal overlapping bolt area) to prevent tampering with the bolt.

(4) Exterior doors should have steel frames.

(5) Hingepins should contain security set screws or pins to prevent removal.

(6) Peened or welded hingepins should be the standard, not the exception.

e. Windows and other openings.

(1) Ventilation openings should be secured by security screens or bars.

(2) All ground level windows on equipment storage buildings, toolrooms, supply rooms, and other high value storage areas should have security screening of 6-gauge steel mesh with 2-inch diamond grids or steel bars not more than 4 inches apart with horizontal bars welded to vertical bars so that openings do not exceed 32 square inches.

(3) Use of IDS/CCTV should be considered for critical and sensitive areas/structures. (See chapter 7 and appendix M.)

f. POL security.

(1) Filler caps to bulk fuel and oil storage tanks should be secured with case hardened steel security type padlocks or equivalent devices.

(2) The electrical power switch to all electric-operated gas pumps are generally left unmarked and are located inside a secured area. Switches are normally turned off during nonduty hours.

(3) Nozzles to gas pumps should be locked with case hardened steel locks/padlocks when not in use.

(4) All POL items (gas, diesel and oil) should be locked during nonduty hours.

g. Vehicle security.

(1) Vehicles should be secured at the close of business daily, on weekends and holidays, or when vehicles are to be left unattended/unoccupied. Minimal vehicular security should include the following:

(a) Apply emergency brake.
(b) Place transmission in "Park" position.
(c) Lock steering column/transmission and remove key from vehicle.
(d) Raise all windows to their maximum upward positions.
(e) Remove all extraneous and unmounted property from vehicle (such as radios, equipment, instruments, tools, etc.).
(f) Lock all doors, windows, compartments, hatches, trunks and gas tanks.

(2) Where possible, all vehicles should have lockable gas caps and be parked in a fenced, well-lighted area. Vehicles may be parked in secured engineer equipment storage yards, post motor pools, and other secured US Government agency motor pools or commercial parking areas that have on-duty attendants, provided an agreement is made with the supporting activities.

(3) Privately owned vehicles should not be parked in Engineer motor pools/maintenance areas/equipment storage yards.

(4) Vehicle keys and US Government credit cards must be secured at all times in **separate heavy metal locked cabinets/safes** when vehicles are not on dispatch. Credit cards must be secured by the operator at all times while vehicle is on dispatch and will not be left in vehicle when unattended. All credit cards must be inventoried quarterly by serial number by a disinterested person; and a written record must be retained for 2 years. Any loss/discrepancy must be reported immediately to the security officer.

16-18 Offices, Warehouses, Etc.

Corps of Engineers **resident/project engineer offices, warehouses, compounds and auxiliary facilities** are operated throughout the world to provide administrative, technical, and logistical support for the various Corps of Engineers projects cited previously. They provide points of contact for assistance to public users of Corps facilities and recreation areas, and provide ranger support for recreational areas with responsibility for liaison with civil law enforcement and federal investigative agencies.

a. The general public should be made to feel welcome; however, their access should be limited to controlled areas. Direct assistance may be provided under emergency conditions when they occur if security aspects are not compromised. Indirect assistance, such as telephonic guidance/direction, etc., will be provided when security aspects are unclear or unknown.

b. Security measures for these facilities are the same as defined for land plant facilities in paragraph 16-17.

c. Warehouses/storerooms where **nice-to-have/high-value Government property** is stored, should require as a minimum, the following additional security requirements:

(1) Exterior doors equipped with security type mortise locksets, series 1000 (86) with 1-inch throw or case hardened steel hasps and case hardened steel security padlocks. Locks rotated semi-annually and recorded on the key control register.

(2) All small high-value items secured in locked containers/cages/room within the warehouse.

(3) Access restricted to responsible persons.

(4) Windows covered by security mesh or equivalent aesthetic material.

16-19 Construction Projects

a. Corps of Engineers military and civil works construction projects are designed and supervised by Corps personnel for execution by civilian contractors throughout the world. **During construction, the contractor has worksite security responsibility,** including Government furnished materials on-site, until accepted by the using agency.

b. Site security considerations:

(1) Presite security conference will be conducted by key installation personnel, the district security officer, and contractor personnel.

(2) Follow-up inspections conducted as required.

(3) Schedule and inventory arrival of equipment and materials in construction priority.

(4) Secure storage areas and facilities (such as semitrailers).

(5) Protective lighting/fencing.

(6) Security forces and auxiliary equip ment and liaison with local law enforcement agencies.

(7) Contractor and subcontractor employee identification.

(8) Separate employee and project vehicle parking/registration procedures.

(9) Post-construction inventory of materials by a Corps of Engineers representative.

c. Tool and equipment security:

(1) Gang boxes secured with case hardened hasps and locks.

(2) Color code/marking of all tools/equipment.

(3) Frequent inventories/inspections by supervisory personnel.

d. For buildings, vehicles and equipment security, see land plant security considerations, paragraph 16-17.

e. Security of explosives:

(1) Military projects secured IAW AR 190-11.

(2) Civil works projects secured IAW Title XI, Regulations of Explosives (P.L.91-452) and part 181, Title 26, Code of Federal Regulations. Corps of Engineers on-site representative should immediately notify the district security officer when explosives are to be stored on-site. The physical

security officer then should conduct a physical security inspection, preferably with representatives assigned to the Bureau of Alcohol, Tobacco, and Firearms (ATF).

(3) The CFR prescribes **minimum** legal standards of explosive security. On-site storage usually requires adding additional requirements to contract specifications for daily issue/turn-in/accountability procedures, security fencing, lighting and watchman services. **Failure to comply could result in explosives being stored off-site by the contractor** at his storage area.

Other Considerations — Section VI

16-20 Control, Warning, And Prohibition Signs

Proper and strategic selection of sign locations will assist greatly in external security measures.

a. Control signs.

(1) Used to regulate foot and motor vehicle traffic at entrances and exits to parking and sightseeing areas near project operational areas.

(2) To regulate visitors to recreational and wildlife management areas.

b. Warning/prohibition signs.

(1) Displayed in accordance with established policy.

(2) Displayed in areas noticeable to the public and erected according to the degree of security desired or criticality of project operation.

c. Water release horn at dams will be specified on signs conspicuously located to warn the public of rush waters (figure 96).

d. Sign criteria.

(1) AR 190-13.

(2) AR 380-20.

(3) Internal Security Act 1950.

(4) Appropriate engineer regulations.

16-21 Support Agreements

a. Written agreements should be prepared, coordinated, and maintained by the project manager with appropriate state police, and local police authorities when special support requirements are necessary.

b. Agreement considerations:

(1) Authority-local authorities jurisdiction.

(2) Response during routine and emergency situations.

(3) Communication checks.

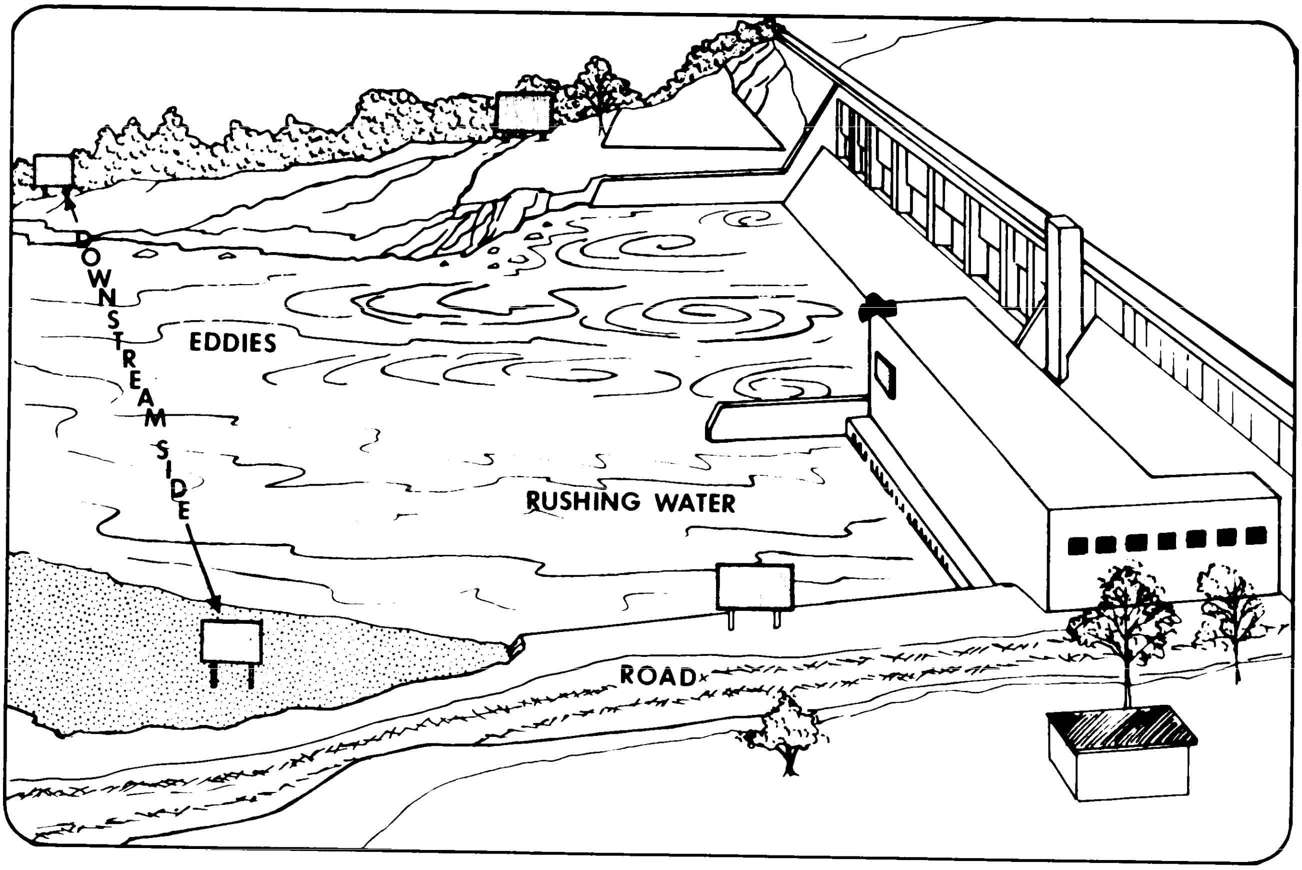


Figure 96—Correctly placed release horn warning signs below a dam.

(4) IDS interface.

(5) Emergency Equipment.

16-22 Visitor Registers

Visitation room sign-in/sign-out registers should be reviewed every 6 months by security personnel. These can serve as an excellent source for determining visitation patterns involving the same people.

16-23 Visitation Room

a. Should be controlled through IDS and CCTV.

b. Periodically inspected for strange ob-. jects or stay-behind persons.

c. Located to prevent access to critical facilities.

d. Pamphlets or project cut-away charts, if displayed, should not depict access routes or critical functioning areas of the plant, dam structure or facility.

16-24 Impress/Recreation Fee Funds

a. Impress/recreation fee funds should be secured in GSA specified safes or vaults.

b. Safes or vaults should be secured to a permanent structural fixture.

c. Money should not exceed amounts outlined in appropriate regulations (AR 190-13, AR 37-103, AR 37-103-1, ASPR 3-607.2(c)), and appendix L of this manual.

16-25 Contingency Plans

The following points should be covered in all contingency planning:

a. Plant and facility evacuation.

b. Public warning in case of actual or possible dam rupture.

c. Response force:

(1) Airmobile

(2) Motor vehicle

(3) Foot.

d. Isolation of public during hazard conditions (extended rains, etc.).

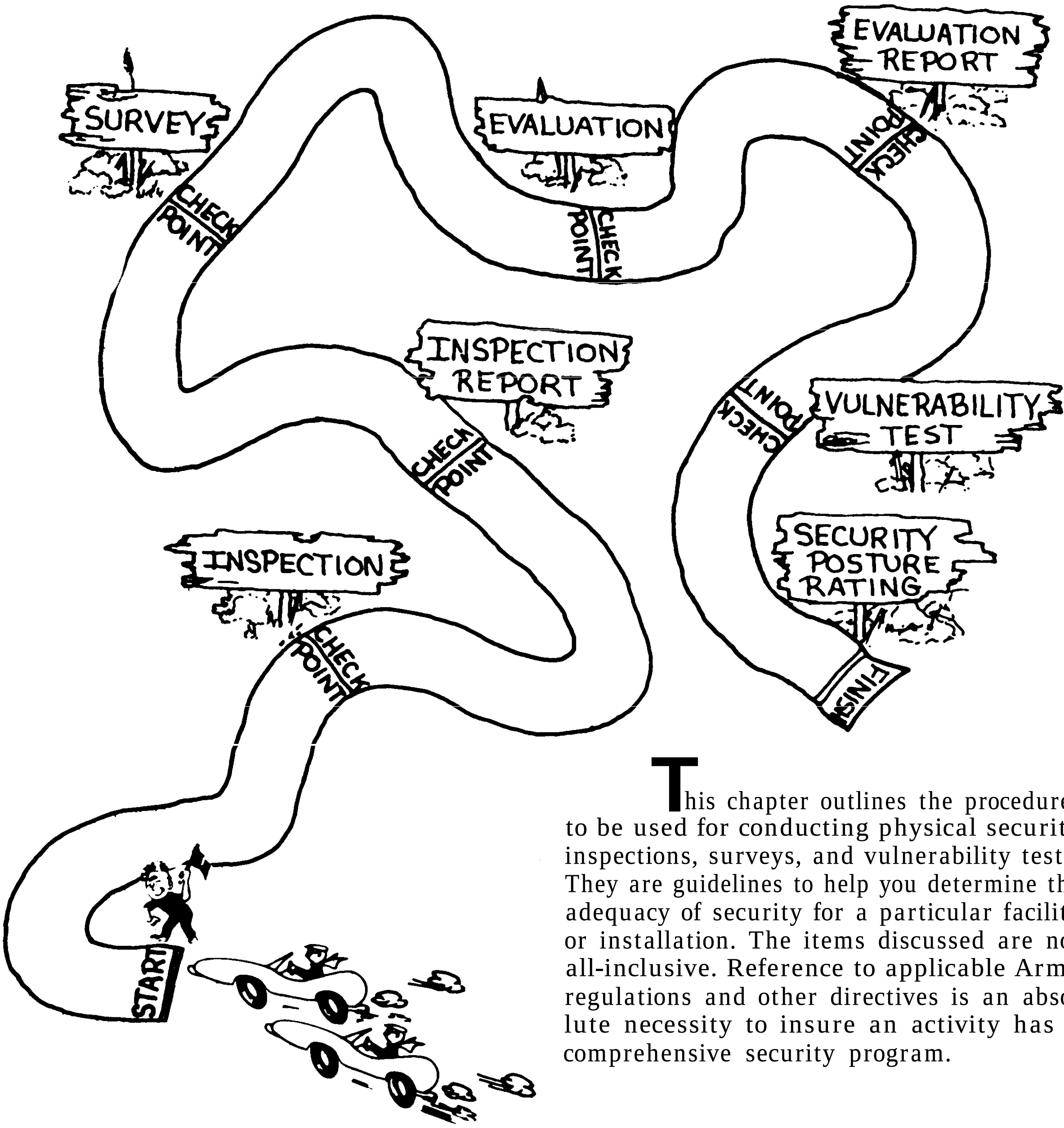
e. Investigating/reporting of crimes against persons and property, fraud and conflict of interest.

f. Pursuit operations.

g. Bomb threats.

Chapter 17

Security Analysis and Evaluation



This chapter outlines the procedures to be used for conducting physical security inspections, surveys, and vulnerability tests. They are guidelines to help you determine the adequacy of security for a particular facility or installation. The items discussed are not all-inclusive. Reference to applicable Army regulations and other directives is an absolute necessity to insure an activity has a comprehensive security program.

17-1 Basic Guidelines

Physical security inspections are only conducted at Department of Army installations, activities, and facilities. The types of inspections most often conducted are initial annual, biennial, and supplemental. Inspection personnel should be trained in accordance with AR 190-13. Inspections are most often required on a biennial basis.

Missions of some activities on an installation may be exempt from inspection and be inspected under guidance of regulations and directives unique to those activities.

17-2 Coordination

a. Liaison and coordination should be established with other agencies on the installation prior to inspection.

b. The director of facility engineers can provide information to benefit the overall security program.

c. Other agencies, such as MI (threat analysis) and ASA have input essential to the security program.

17-3 Security Library

a. A security library is necessary to aid people in preparing for and conducting inspections.

b. Inspectors, to be effective, should know the mission and history of each activity they are going to inspect.

c. Previous inspection reports will be reviewed and assessed to guide inspectors through a follow-up inspection prior to the regular inspection (of arms rooms, for example).

d. A file of all appropriate SOP, Army regulations and training and doctrinal manuals will be maintained and be accessible to inspectors. Security libraries should contain the latest data on items of security interest, e.g., color copiers, which can be used to duplicate government bonds similar to originals, etc.

17-4 Entrance Interviews

a. Entrance interviews are usually required prior to conducting the actual inspections.

b. The conduct of the inspection will act as a service to the commander or supervisor.

c. All members of the inspection team will be introduced and the purpose and objectives of the inspection outlined.

d. Assistance and cooperation by the commander, supervisor, and inspecting party will be stressed.

e. Avoidance of unusual terminology is a must.

f. A review of waivers, work orders, and exceptions is a must prior to conducting the inspection.

g. Anticipating changes to the unit's mission should be considered by inspectors and the details worked out by all personnel concerned.

17-5 Conducting Inspections

The established inspection plan should start with the inspection being conducted from the outside to the inside of the facility, activity, or area.

- Observation of the unit will be conducted during all hours of unit operation.
- Interviews of managerial and operational personnel will be performed.
- Security forces should be inspected so as not to disrupt the mission.
- A class assessment should be made of security force training, especially if security knowledge is inadequate.
- Inspection of entry and movement control should not hinder operations.
- All communications (alternate or primary, base or handheld) should be thoroughly inspected.
- Each inspector should take detailed notes and have a checklist ready as a reference.

17-6 Exit Interviews

a. Exit interviews should be conducted as soon as possible after the inspection, and the inspection's goal and objectives should be restated.

b. The commander should be informed of all deficiencies and compliments noted in an effort to establish a good relationship.

c. A rating on the results of the inspection should be provided during the exit interview.

d. Recommendations should always be realistic and positive.

e. When considering recommendations, the mission, budget limitation, threat, resource availability and urgency must be considered.

f. Written reports should be forwarded through channels within 30 days and follow-up corrective action initiated within the prescribed time frames.

17-7 Report (DA Form 2806)

Physical Security Survey, DA Form 2806, is used for survey and inspection reports. AR 190-13 governs use of the form. Details on completion of the form can be found in FM 19-10, and in appendix T, pp. 428 and 429 of this manual.

Surveys and Evaluations

Section II

17-8 Surveys

A physical security survey differs from an inspection in that a survey covers a formal assessment of an installation activity. Each survey includes a complete reconnaissance, study and analysis of installation property and its operations.

153-846 0 - 94 - 12

17-9 Survey Report

The survey report on DA Form 2806 is completed in the same manner as an inspection report.

Exhibits to the survey report will be handled IAW AR 190-13.

June 30 is the deadline for submission of one copy of the installation's physical security survey.

17-10 Evaluations

An evaluation of an installation's security posture will be based on this manual. A security list should be prepared, assigning priorities for allocation of security resources.

17-11 Vulnerability Tests

a. It is essential that vulnerability tests be conducted to assess operational security alertness and posture.

b. When conducting a vulnerability test, specific objectives should be stated and complied with (safety, etc.).

c. Security personnel who check identification must detain unauthorized persons; conduct preliminary searches on suspects; enforce security procedures; and report any security violations.

d. Unauthorized disclosures of information by members of the security forces should be detected and immediately reported.

e. Detailed planning should be conducted prior to implementing a vulnerability test and priority of targets be established accordingly.

f. Personnel selected to conduct vulnerability tests should meet all the criteria required for the test and have appropriate material and equipment to conduct the tests.

g. Each test team should be briefed on all instructions pertaining to execution of the test.

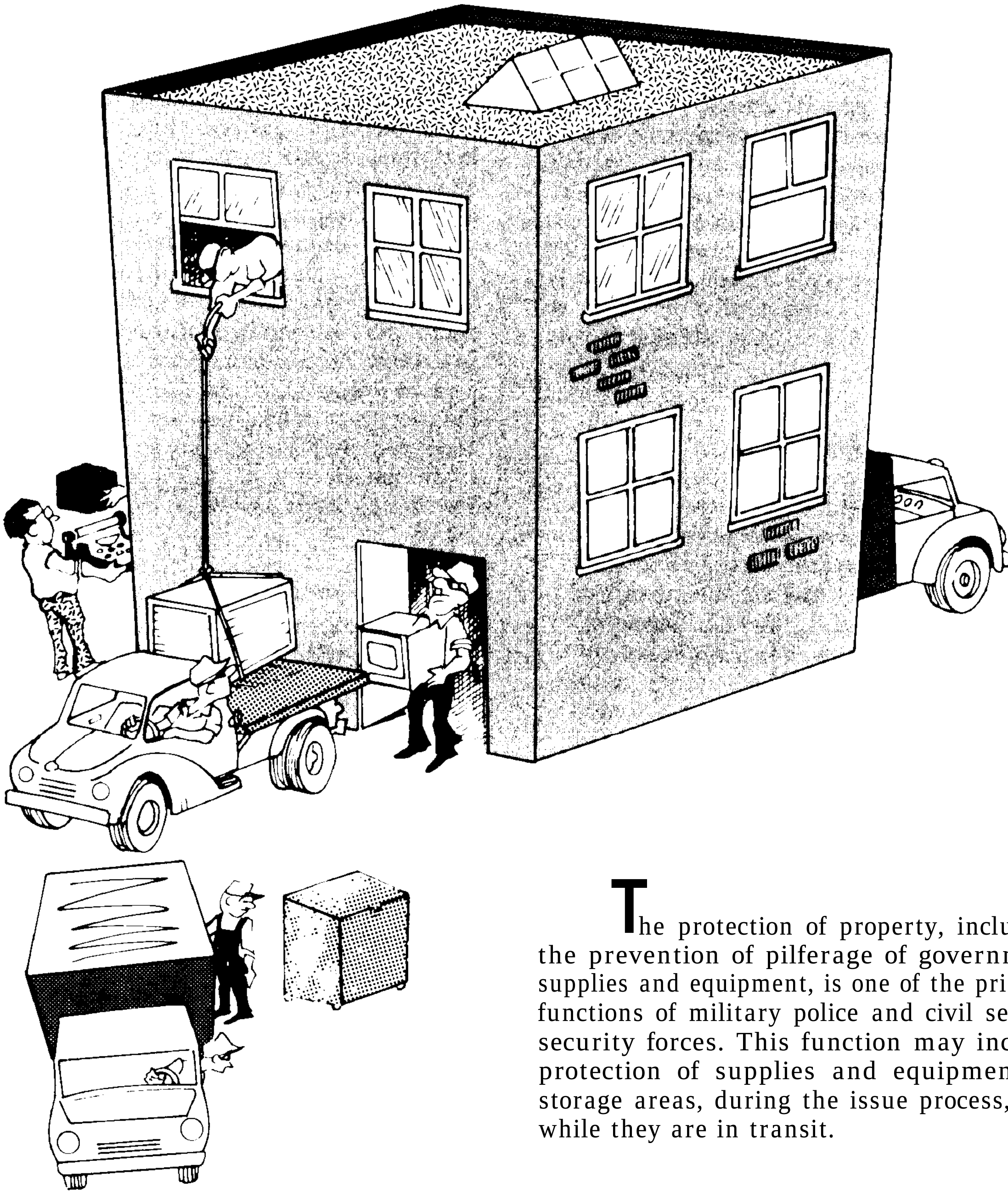
h. A means for neutralizing escorts should be devised in the interest of security.

i. Procedures should be used to simulate planting of sabotage devices to add realism to tests.

j. A written report will be provided on the results of each vulnerability test and will be given the proper rating.

Appendix A

Pilferage



The protection of property, including the prevention of pilferage of government supplies and equipment, is one of the primary functions of military police and civil service security forces. This function may include protection of supplies and equipment in storage areas, during the issue process, and while they are in transit.

A-1 Pilferage

a. Pilferage is probably the most common and annoying hazard with which security personnel are concerned. It can become such a financial menace and detriment to operations that a large portion of the security guard force efforts may have to be devoted to its control. Pilferage, particularly petty pilferage, is frequently difficult to detect, hard to prove, and dangerous to ignore.

Note: The words, "pilfer," "pilferer," and "pilferage" are used throughout this manual in the senses in which they have come to be accepted by physical security personnel rather than in the dictionary sense. Thus, they include the meanings of "steal," "thief," "theft," "larceny," and similar terms. They embrace not only petty theft, but theft of any quantity or monetary value. (For a discussion of pilferage in consumer outlets and associated storage facilities, see section III of this appendix.)

b. It is imperative that all military personnel, to include the management, understand the potential losses to the military on a daily basis.

c. Yearly, military installation property loss throughout the world would increase millions of dollars each year if subjected to uncontrolled pilferage. However, the risks incurred cannot be measured in terms of dollars alone. Loss of critical supplies for tactical units could result in unnecessary loss of life and danger to national defense. In some areas, losses could assume such proportions as to jeopardize the mission of the installation. All installations and facilities can anticipate loss from pilferage. Actual losses will depend on such variable factors as type and amount of materials, equipment, and supplies produced, processed, and stored at the facility; numbers of persons employed; social and economic conditions in surrounding communities; command attitudes (this is a most important consideration); and physical security measures employed. Because these factors differ greatly in various types of installations and in different geographical locations, each must be considered separately.

d. To determine the severity of this hazard at any given installation or facility, there is a need to determine the amount of loss which may be occurring. Unfortunately, this is not always an easy task. Accounting methods may not be designed to pinpoint thefts; consequently, such losses remain undisclosed or they are lumped together with other shrinkages, thus effectively camouflaging them.

e. One of the most common inventory methods is to conduct periodic inventories of property and assume that unaccounted-for inventory loss is due to theft. This is, a convenient but deceptive and dangerous device because theft is only one of many causes of inventory shrinkage.

f. Failure to detect shortages in incoming

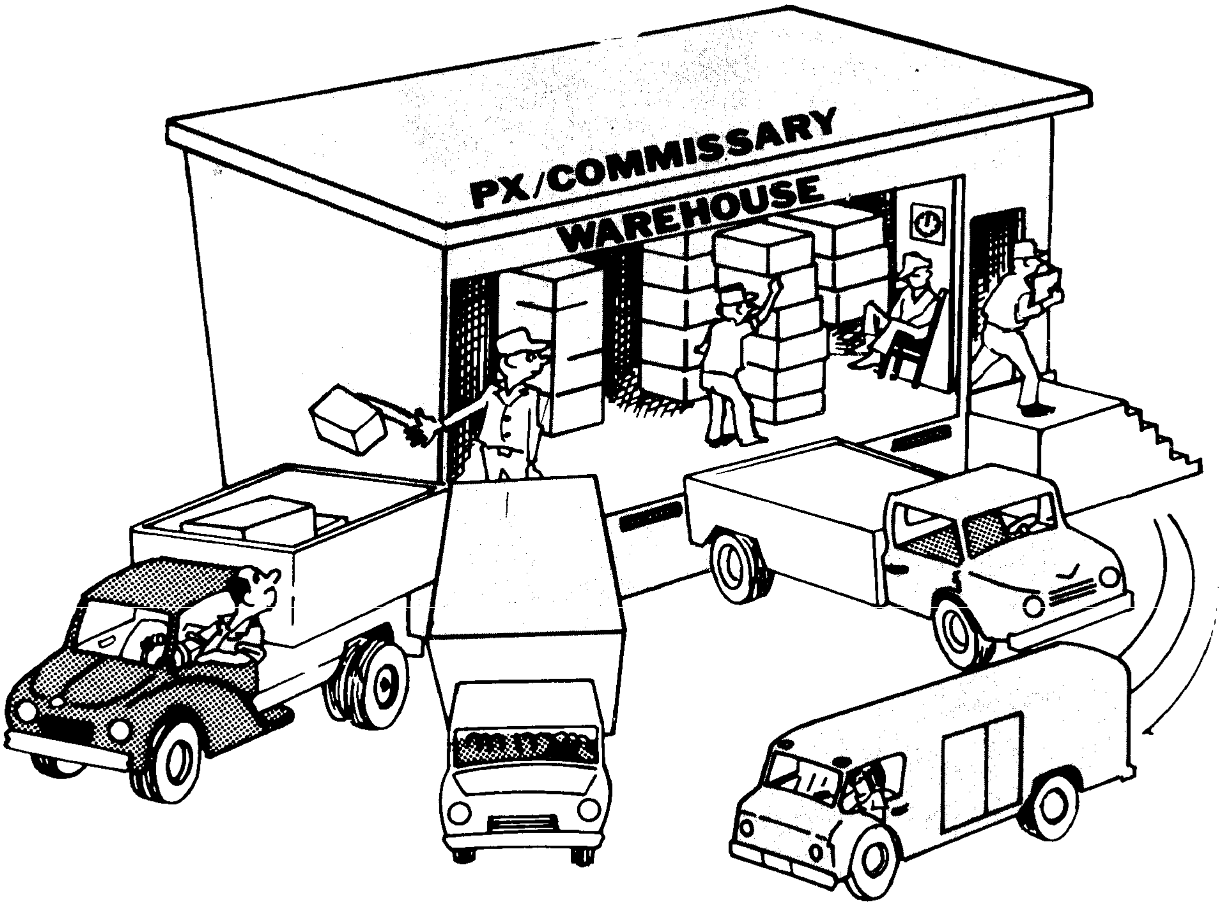


Figure A-1—When shipping and receiving is mismanaged, entire loads of supplies, material, and foodstuffs may be taken.

shipments, improper stock usage, poor stock accounting, poor warehousing, improper handling and recording of defective and damaged stock, and inaccurate inventories cause inventory losses that may be inaccurately labeled as pilferage.

g. In some cases inventory losses may be impossible to detect because of the nature and quantities of materials involved. Stock inventory records may not be locally maintained, or there may be no method for spot checks or running inventories to discover shortages.

(1) This is an undesirable situation and should be corrected where possible. Recommendations should be made that running inventories be maintained.

(2) An established estimate of the degree of severity of this hazard may have to be revised because of anticipated changes in the economic or social conditions in nearby communities, increases in numbers of employees, introduction of new materials into the installation, or any of the other



Figure A-2—The systematic pilferer steals according to plan.

variable factors on which estimates of expected losses are based.

(3) The degree of risk involved can be determined only by analysis of the relative vulnerability of each area or activit y of the installation to the hazard of pilferage. To do this, it is necessary to consider the problem of who is likely to steal, and what items they are most likely to take (see Risk Analysis, paragraph 1-6).

A-2 Profile of Pilferers

There are two types of pilferers who physical security personnel must be prepared to counteract—or at least recognize so proper physical security measures may be taken to afford the best protection against them. These are **casual pilferers** and **systematic pilferers.**

a. A **casual pilferer** is one who steals primarily because he is unable to resist the temptation of an unexpected opportunity and has little fear of detection. There is usually little or no planning or premeditation involved in casual pilferage and the pilferer **normally acts alone.** He may take items for which he has no immediate need or foreseeable use, or he may take small quantities of supplies for use of family or friends, or for use around his home. The **degree of risk involved in casual pilferage is normally slight** unless very large numbers of persons are involved.

(1) Casual pilferage occurs whenever the individual feels the need or desire for a

certain article and the **opportunity to take it is provided by poor security measures.** Though it involves unsystematic theft of small articles, casual pilferage is nevertheless very serious, and it may have a great cumulative effect if permitted to become widespread—especially if the stolen items have a high cash or potential value.

(2) There is always the possibility that casual pilferers, encouraged by successful theft, **may turn to systematic pilferage. Casual pilferers are normally employees** of the installation and usually are the most difficult to detect and apprehend.

b. A **systematic pilferer** is one who steals according to **preconceived plans,** and steals any and all types of supplies to **sell for cash or to barter** for other valuable or desirable commodities.

(1) He may work with another person or with a well-organized group of people, some of whom maybe members of a cleaning team or even be in an advantageous position to locate or administratively control desired items, or remove them from storage areas or transit facilities.

(2) The act of pilferage maybe a one-time occurrence, or such acts may extend over a period of months or even years. Large quantities of supplies, with great value, may be lost to groups of persons engaged in elaborately planned and carefully executed systematic pilferage activities.

(3) Systematic pilferers may or may not be employees of the installation; if they are not, they frequently operate in conspiracy with such employees.

A-3 Motivations of Pilferers

The degree of dishonesty may vary with the motivation of pilferers. The uses pilferers make of pilfered items and/or the money from them does not establish any patterns. In fact, their modus operandi is difficult to detect due to their changing motivational desires.

a. The military or civilian thief may:

- ❑ Not be profit oriented
- ❑ Be any person
- ❑ Operate with others

b. Usually, the common danger signs that a pilferer is at work are:

- Dedication and devotion to work
- Increase in personal financial spending
- Refusal to accept office, activity or installation movement control procedures

c. A pilferer's rationalization to dishonesty is:

(1) Why not, others are doing it
(2) It's morally right to me
(3) "It's not stealing, only borrowing."

d. Elements that induce dishonesty:

(1) Target of opportunity
(2) High personal need or desire
(3) Rationalization of personal actions.

A-4 Opportunities For Pilferage

Pilferage may occur anywhere. Even supplies that are stationary in permanent or semipermanent storage areas or warehouses are vulnerable to theft if adequate precautionary measures are not taken; and vulnerability increases as supplies become more mobile.

a. New and greater opportunities for pilferage are present when supplies are being transported in trucks, trains, planes, or ships.

b. The greatest vulnerability and the widest variety of opportunities occur at the various points where supplies are transferred from one means of transportation to another,

or from storage to transportation and vice versa.

c. Remember that anyone maybe a pilferer. Where need or desire exists, and opportunity is presented, theft is almost sure to result.

A-5 Targets for Pilferage

Both the casual and systematic pilferer have certain problems to overcome in order to accomplish pilferage objectives. Some of these are:

a. A pilferer's **first requirement is to locate the item or items to be stolen.** For the casual pilferer this may be accomplished through individual search or even accidental discovery. In systematic pilferage, more extensive means are generally employed. These may consist of surveillance by members of the group, or checking of shopping and storage areas or documents by those who have access to them.

b. The **second requirement is to determine the manner in which he can gain access to and possession of the desired items.** This may involve something as simple as breaking open a box. Or it may be as complex as surveying security factors such as physical safeguards or security procedures for weaknesses, attempting to bribe security forces, altering or forging shipping documents or passes, or creating disturbances to divert attention of security personnel while the actual theft is taking place.

c. The **third requirement is to remove the stolen items** to a place where the thief may benefit from his act. Articles of clothing may be worn to accomplish this. Small items may be concealed in any of many possible places on the body of the thief or in vehicles. Through falsification of documents, whole truckloads of supplies may be removed from their proper place without immediate discovery.

d. Finally, to derive any benefit from his act, the pilferer **must use the item himself or dispose of it** in some way. The casual pilferage of supplies is intended primarily to satisfy the need or desires of the thief. The systematic pilferer usually attempts to sell the material through "fences," pawnbrokers, or black market operations.

(1) Detection of use or disposal can help prevent similar pilferage through investigation and discovery of the means used to accomplish the original theft. Similarly, **each of the problems faced by would-be pilferers offers opportunities for constructive preventive measures.** Careful study of the possible opportunities for the pilferer to solve his problems is essential in security work (see Risk Analysis, paragraph 1-6).

(2) The **primary concern of a systematic pilferer in selecting a target is its monetary value.** Since he steals for personal profit, the systematic pilferer looks for items from which he can realize the greatest financial gain. This means he must also have or be able to find a ready market for items he maybe able to steal. He pilfers small items of relatively high value, such as drugs, valuable metals or electronic items, including radio and television tubes. However, we cannot discount the possibility that a systematic pilferer may, if the profit is substantial, select a target of great size and weight. As a rule, bulk storage areas contain most of the material that may be selected by systematic pilferers.

(3) The **casual pilferer is likely to take any item easily accessible to him.** Since he normally will remove the item from the installation by concealing it on his person or in his privately owned automobile, size is also an important consideration. Monetary value and available markets are not of any great concern to the casual pilferer, because he usually does not have any idea of selling the property he steals.

(a) He normally uses the item himself. Any property not secured or not under surveillance, and small enough to be hidden on the person or otherwise removed from the installation by commonly available means, is subject to casual pilferage.

(b) Storage areas containing loose items are more likely to tempt casual pilferers than bulk storage areas.

A-6 Methods of Pilferage

There are many ways by which pilfered items may be removed from military installations. Because the motives and targets likely to be selected by systematic and casual pilferers are very different, the methods of operation for each are very different.

a. As stated above, the casual pilferer steals whatever is available to him and generally removes it from the installation by concealing it on his person or in his automobile.

b. The methods of the systematic pilferer are much more varied and complex. The means he may employ are limited only by his ingenuity. The following are cited as examples:

(1) Shipping and receiving operations are extremely vulnerable to systematic pilferage. It is here that installation personnel and truck drivers have direct contact with each other and readily available means of conveyance. This offers a tempting opportunity for collusion. Although most truck drivers and employees are honest, a few of them may succumb to temptations such as a receiving clerk who certifies the receipt of property that the truck driver actually disposed of prior to his arrival at the installation. An installation employee can provide property to a truck driver and assist in concealing it aboard the truck for unauthorized removal from the installation. Employees can assist truck drivers in removing property by executing fictitious invoices that appear to be legitimate when inspected by security personnel.

(2) One individual must not have control of all shipping and receiving transactions. Obviously this procedure invites manipulation of Government bills of lading and inaccurate storage and movement procedures through failure of one activity to compare bills and invoices with another activity. The opportunities for monetary kickbacks increase without a sound system of checks and balances.

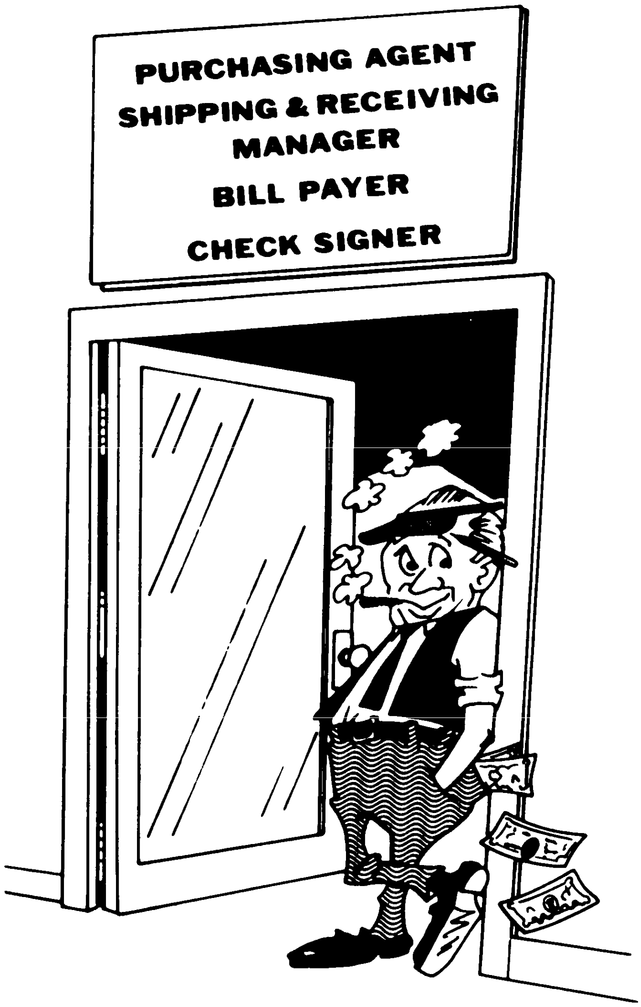


Figure A-3—One-person control invites losses.

(3) Railway employees assigned to switching duties on the installation can operate in a similar manner but with more difficulty because a railway car normally cannot be directed to a location where stolen property can be easily and safely removed. Additional confederates are usually required to transfer stolen goods from a railway car, at some point or siding outside the installation, into some other means of transportation for removal. This increase in the number of persons involved reduces profits and increases the chances for discovery and apprehension.

(4) Tanker trucks employed for ship ment of petroleum products maybe altered to permit pilferage of the product.

(5) Trash disposal and salvage disposal activities offer excellent opportunities to the systematic pilferer to gain access to valuable material. Property may be hidden in waste material (Fig A-2) to be recovered by a confederate who removes trash from the installation. Serviceable or even new items of equipment or material may be classified as salvage by dishonest employees operating in collusion with other persons working in or having access to salvage disposal.

c. Other methods which maybe employed by systematic pilferers to remove property from military installations include throwing items over fences to be retrieved at a later time by themselves or by confederates; packaging property and sending it to outside addresses through mail channels; collusion with security personnel; loose fitting clothing that can be worn to conceal small items; and removal of items on vehicles belonging to outside contractors and vendors.

A-7 Control Measures For Casual Pilferage

Specific measures for preventing pilferage must be based on careful analysis of the conditions at each installation. The most practical and effective method for controlling casual pilferage is to establish psychological deterrents. This may be accomplished in a number of ways. Some are discussed in the following paragraphs.

a. One of the most common means of discouraging casual pilferage is to **search individuals and vehicles** leaving the installation at unannounced times and places.

(1) Spot searches may occasionally detect attempts of theft but greater value is realized by bringing to the attention of all employees they may be apprehended if they do attempt to illegally remove property.

(2) Care must be taken to insure that personnel are not demoralized nor their legal rights violated by oppressive physical controls or unethical security practices.

b. An **aggressive security education** program (chapter 3) is an effective means of convincing employees that they have much more to lose than to gain by engaging in acts of theft. Case histories may be cited where employees were discharged or prosecuted for pilferage. Care must be taken in discussing these cases to preclude identification of individuals, because of possible civil suits for defamation of character. Also, it is generally poor policy to publicize derogatory information pertaining to specific individuals. It is important for all employees to realize that pilferage is morally wrong no matter how insignificant the value of the item taken.

c. It is particularly important for supervisory personnel to set a proper example and maintain a desirable moral climate for all employees.

d. All employees must be impressed with the fact that they have a responsibility to report any loss to proper authorities.

e. Adequate inventory and control measures should be instituted to account for

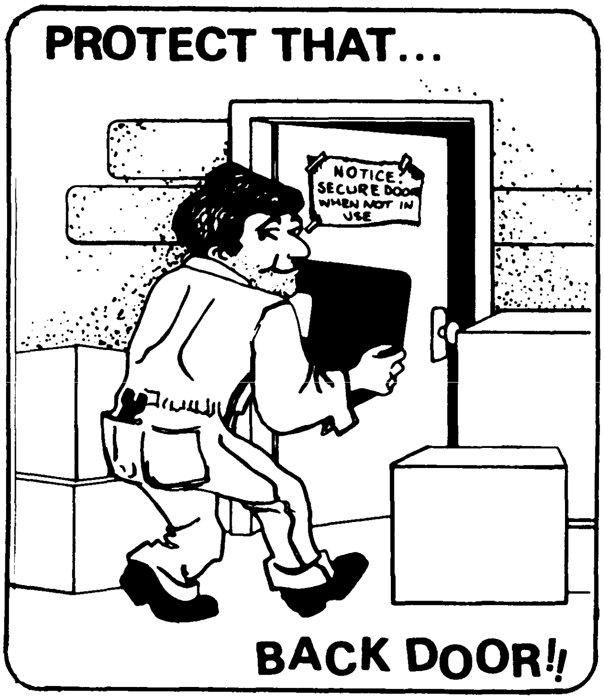


Figure A-4—Good physical controls discourage casual pilferage.

all materiel, supplies, and equipment. Poor accountability,if it is commonly known, provides one of the greatest sources of temptations to the casual pilferer.

f. Identification of all tools and equipment by some mark or code (where feasible) is necessary so that government property can be identifiable. Installation tools and euqipment have counterparts on the civilian economy and cannot otherwise be identified as government property. Another control method is to require signing for all tools and equipment to be used by individuals. The use of the signature control method reduces the temptation to pocket the item.

g. In establishing any deterrent to casual pilferage, physical security officers must not lose sight of the fact that **most employees are honest** and disapprove of thievery. Mutual respect between security personnel and other employees of the installation must be maintained if the facility is to be protected from other more dangerous forms of human hazards. Any security measure that infringes on the human rights or dignity of others will jeopardize, rather than enhance the overall protection of the installation.

A-8 Control Measures For Systematic Pilferage

Unlike the casual pilferer, the systematic thief is not discouraged by psychological controls. Nothing short of active physical security measures are effective in eliminating losses from this source. Some of these measures include:

a. Establish security surveillance of all exits from the installation.

b. Establish an effective package and material control system.

c. Locate parking areas for private vehicles outside the perimeter fencing of the activity.

d. Eliminate potential thieves during the hiring procedure by careful screening and observation.

e. Investigate all losses quickly and efficiently.

f. Establish an effective key control system.

g. Establish adequate security patrols to check buildings, grounds, perimeter, and likely locations for clandestine storage of property removed from its proper location.

h. Install mechanical and electrical intrusion detection devices where applicable and practical.

i. Coordinate with supply personnel to establish customer identification, to authenticate supply release documents at warehouses and exit gates.

j. Establish appropriate perimeter fencing, lighting, and parking facilities and effective pedestrian, railway, and vehicle gate security controls.

A-9 Audit Procedures

A detailed item/merchandise audit procedure conducted once yearly will greatly assist in detecting pilferers. The audit should provide a thorough review of all handling and accountability procedures and control systems. An audit should be conducted even though an installation or activity has outstanding control measures.

a. An audit will discourage dishonesty and:

(1) Uncover manipulations

(2) Detect control irregularities.

b. For an example of an audit concerning stock withdrawals and warehouse storage, see figure A-5.

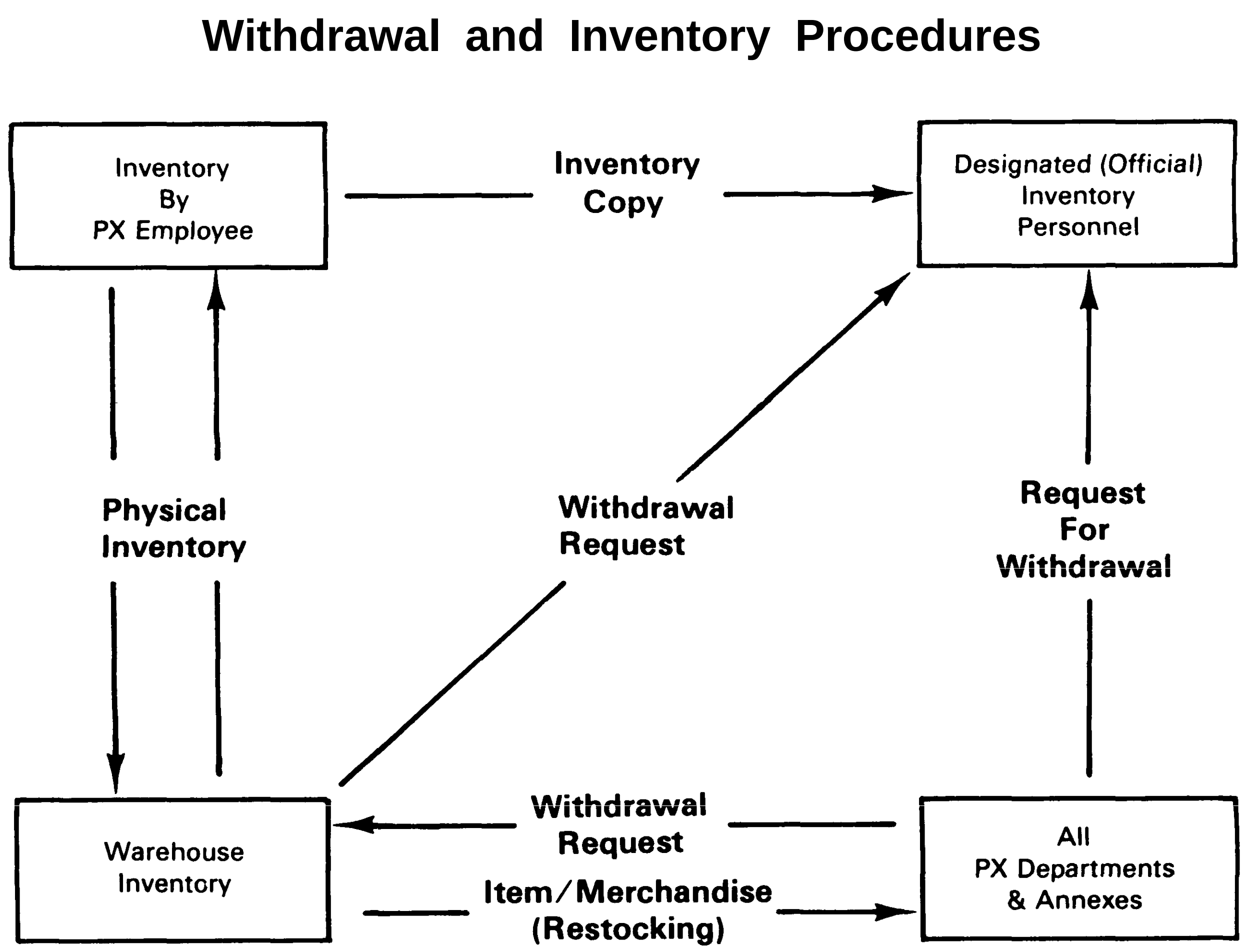


Figure A-5—Sample of audit steps

A-10 How To Stop Employee Theft

No matter what it's called—internal theft, peculation, embezzlement, pilferage, inventory shrinkage, stealing, or defalcation—thefts committed by employees are behind at least 60 percent of crime-related losses. So many employees are stealing so much that employee theft is the most critical crime problem facing business today.

Although employee theft results in part from factors beyond control, the extent of employee theft in any business is a reflection of its management—the more mismanagement, the more theft.

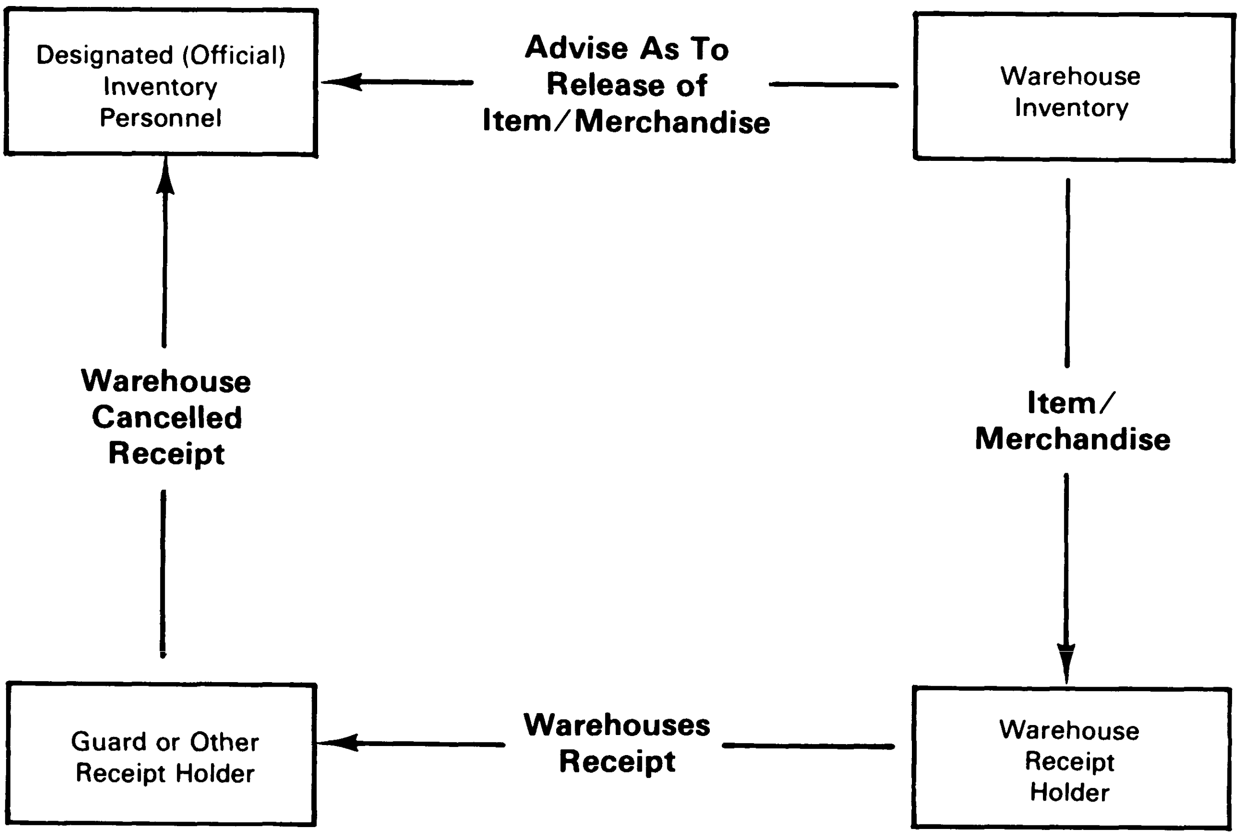
a. An effective stop-employee-thefts policy must include at least the following:

- Preemployment screening.
- Analysis of opportunities for theft.
- Analysis of how employees steal.
- Management-employee communication.
- Prosecution of employees caught stealing.

b. Each employer must reduce losses as much as possible. A police state need not be created. Large monetary expenditures need not be made.

c. Preemployment Screening. The best way to stop employee theft is simply not hire those employees inclined to steal. The best

Warehouse Redemption Procedures



for accountability of merchandise.

way is also impossible. What the employer must do is set up a screening process that will weed out obvious security risks. Many experts believe that personnel screening is the most vital safeguard against internal theft.

Here are some basic guidelines for the employer (because of the legal implications of the process, a separate discussion follows on employee rights and privacy):

- Always have applicant fill out a written application. Be sure that the written application does not discriminate and conforms to any applicable laws.
- Exercise caution when considering ex-convicts for employment. (This is not meant to be a steadfast rule-individual judgments must be made as to degree of rehabilitation.) It is illegal to solicit information about arrest records not leading to convictions.
- Solicit references but keep in mind that those contacted will give favorable opinions. Ask primary references for secondary references. In contacting the latter, make it clear that the applicant did not refer you.
- Always interview. In interviewing, assess the applicant's maturity and values. Observe gestures.
- Use psychological deterrents-inform applicant that your business routinely runs a security check on background, or that fingerprints will be taken. The hope is that the dishonest applicant won't be back.
- Obtain credit bureau reports but only after following guidelines set forth in the Fair Credit Reporting Act.

d. Opportunities, Methods, and Controls. Cases of employee theft have been documented in almost every conceivable phase of business operations—from theft of petty cash to theft of railroad cars. An infinite variety of methods have been used.

(1) Areas most vulnerable:

- ❑ Shipping and receiving.
- ❑ Inventory.
- ❑ Accounting and recordkeeping.
- ❑ Cash, check and credit transactions.
- ❑ Accounts payable.
- ❑ Payroll.
- ❑ Facility storage units.

(2) Methods used:

- ■ Pilferage (one item at a time).
- ■ Cash register theft or alteration of cash register records.
- ■ Issuance of false refunds.
- ■ Use of back door and trash containers.
- ■ Taking advantage of undersupervision.
- ■ Avoidance of package control.
- ■ Embezzlement.
- ■ Check forgery.
- ■ Stealing credit cards.
- ■ Manipulating computers and stealing computer time.
- ■ Night cleaning crews.
- ■ Duplicating keys, or use of master key that is not properly controlled.
- ■ Collusion with outsiders (inflated claim in insurance, for example).

Too many opportunities exist for employees to exploit. Reduce these opportunities and losses will be reduced. Reduce opportunities by control.

(3) Useful controls:

- Randomly spot check all phases of business, in addition to regular, comprehensive audit.
- Check payroll-make sure you're not paying a fictitious or dead employee.
- Take physical inventory seriously.
- Know what you own-be able to identify it.
- Do not allow one employee to perform all functions. Separate receiving, purchasing, and accounts payable. Separate accountants from cash.
- Control payment authorizations.
- Keep blank checks locked, don't presign or use uncoded, unnumbered checks.
- Reconcile cancelled checks with original invoice or voucher.

- Secure exits—restrict employees to one exit. Prevent exit from rear of buildings. Establish strict package control.
- Inspect cash register receipts daily, inspect tape, insure that employee is identified on slips, deposit monies daily.
- Issue identification badges to decrease employee presence in unauthorized areas.
- Simplify red tape—make it harder for the employee to disguise theft.
- Have employee parking away from business establishment.
- Establish usage schedule of supplies to isolate irregularities.

e. Management—Employee Communication. Leadership must be firm yet reasonable. Most employees pattern their values after yours, so a good example must be set. If you expect employees to remain honest, don't cart home office supplies or goods.

(1) Train new employees, advising them of the company's values and the standards by which they will be expected to perform. Explain all security procedures, stressing their importance. Emphasize that any deviations will be thoroughly investigated.

(2) Establish grievance procedures; give your employees an outlet for disagreement; and be receptive to all grievances submitted. Insure that employees are aware of its existence and that no reprisals are taken.

(3) Regularly evaluate employee performance and encourage employees to evaluate management. Unrealistic performance standards can lead either to desperation and anger, resulting in dishonesty; or to get even attitudes. Regularly review salaries, wages and benefits—don't force employees to steal from you.

(4) Delegate responsibility. Unless decision-making exists among lower and mid-levels, there is a tendency for development of an it's-us-against-them attitude. Delegate accountability as well; no decision is valid if it is lost in a buckpassing routine.

Army Property At Local Level — Section II

A-11 Accountability

Proper accountability by commanders and subordinate personnel cannot be overemphasized. To insure accountability of property, commanders must establish, implement, and supervise an installation, activity, or organization security program.

A-12 Vulnerability

a. Weaknesses in security procedures at the installation, activity and organizational level involving military property create vulnerability supported by criminal activity. Criminal activity includes:

- Theft
- Fraud
- Property diversion
- Property manipulation.

b. Commanders and subordinate personnel must conduct a risk analysis and identify military property that must, in the interest of monetary value and mission accomplish-

Recommended Security Measures

Property	Security Plan	Hand Rcpt/ Property Book	Secured by IDS	PS Plan	Inventoried By Reg	Unit Ldrs	PS Off	SDO	Maint Off	Supply Off	Dining Facility Off	CQ	SDNCO (Inspected by)
Arms/Ammunition	X	X	X	X	X	X	X	X	X	X			X
Small Arms	X	X	X	X	X	X	X	X	X	X			X
Explosives	X	X	X	X	X	X	X	X	X	X			X
Communication/ Electronics Equip	X	X	X	X	X	X	X	X	X	X			X
Handtools, Tool Sets/Kits and Shop Equipment	X	X	X	X	X	X	X		X	X			X
Subsistence Items	X	X		X	X	X				X	X		X
Controlled Sub-stances, Precious Metals, Tax-Free Items	X	X	X	X	X	X	X	X		X			X
Accounts	X	X	X	X	X	X							
POL Products	X	X		X	X	X	X	X	X	X		X	
Repair Parts	X	X	X	X	X	X	X		X				
Aircraft	X	X	*	X	X	X	X	X	X				
Vehicles	X	X	***	X	X	X	X	X	X	X		X	X
Towed Weapon Systems/Components	X	X	Com-ponent	X	X	X	X	X	X				
Carriage Mounted Weapon Systems	X	X	X	X	X	X	X	X	X				X
Construction Material	X		*	X		X	X			X			X
Special Issue Clothing-CTA	X	X	X	X	X	X	X	X			X		
Individual Clothing and Equipment	X	X	X	X	X	X		X		X			
Organizational Equip/Components	X	X	*	X	X	X	X	X	X	X		X	X
Compasses, Bin-oculars, Flashlights	X	X		X	X	X	X			X			X
Medical Unique Items	X	X	X	X	X	X	X	X		X			X
Housekeeping Sup-plies and Equipment	X	X	X	X	X	X				X		X	
Housing Furniture	X	X		X	X	X				X		X	
Mess Equipment	X	X	X	X	X	X	X			X	X		X
Office Machines	X	X	X	X	X	X	X			X			X
Expendable/Con-sumable Supplies	X		X	X	**	X		X		X	X		X

* Depending on facility availability and cost effectiveness
**Depending on local policy
***See par. A-13

Figure A-6—Recommended security measures for Army property.

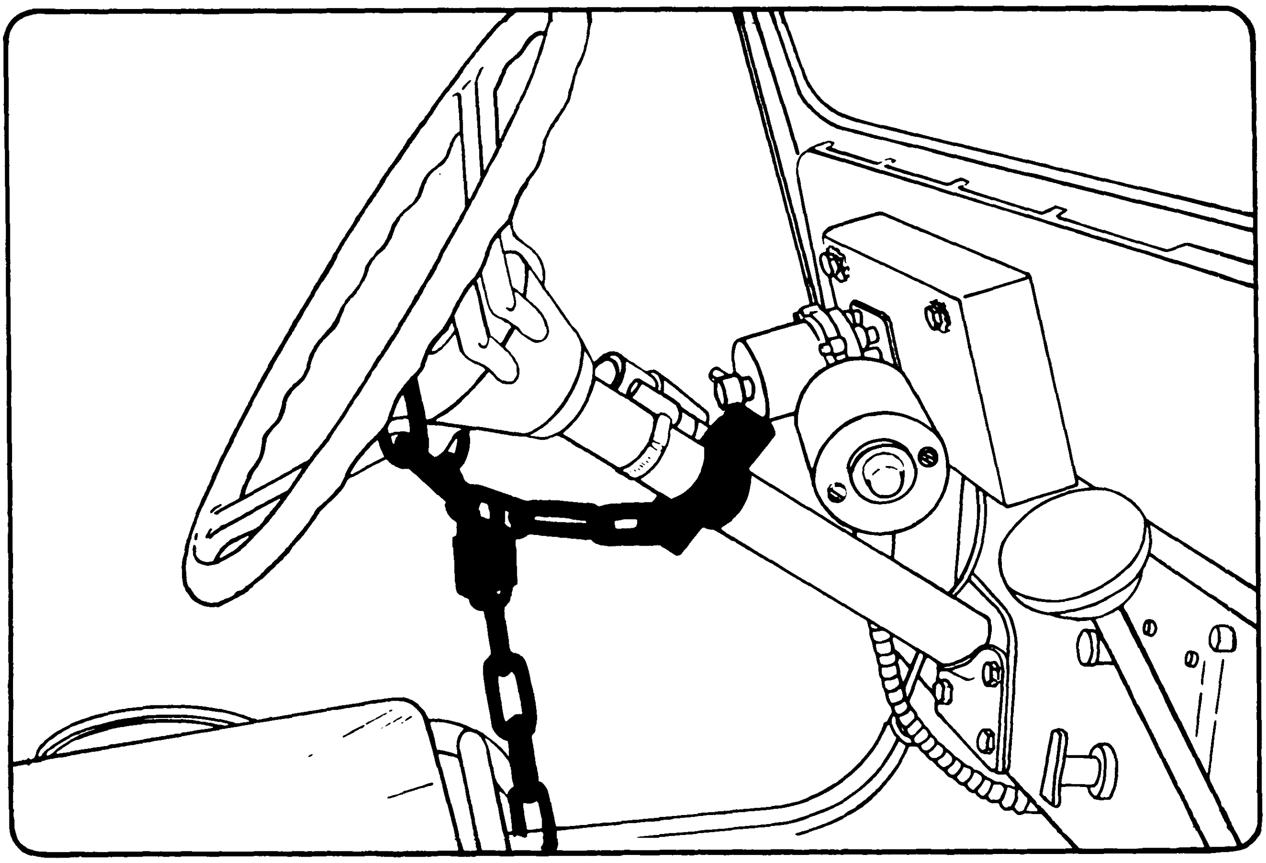


Figure A-7—Typical clamp and chain installation.

ment, design mandatory security measures for specific property.

c. Security doctrine as outlined in this manual should be used to the maximum extent in securing Army property vulnerable to theft, destruction, and/or manipulation.

d. Certain categories of property shown in figure A-6 must be assessed for security vulnerability and protective treatment. Security protective measures addressing this military property should be documented in the unit/installation physical security plan. If the security measures recommended in figure A-6 are implemented using established doctrine, they should eliminate or reduce property vulnerability. This will reduce the incidents of theft, pilferage, and manipulation at the unit/installation.

A-13 Motor Vehicles

a. Security of **tactical vehicles** should be based on a uniform and cost effective approach. For example, to insure proper security of a tactical ¼-ton, 4x4, install a clamp, chain, and lock device as illustrated in figure A-7. To properly install the security device while maintaining safety, use Technical Bulletin (TB) 9-2300-422-20, dated 17 October 1977.

b. Army motor vehicle security should also incorporate at least the use of the following:

❑ Key/lock security and accountability.
❑ Protective lighting.
❑ Fencing.
❑ Walking patrols, as appropriate.
❑ Frequent observation and visits by mobile patrols or unit personnel, such as CQ, SDO, SDNC, etc.

No matter what it's called—internal theft, embezzlement, inventory shrinkage, stealing, or pilferage—thefts committed by employees in consumer outlets contribute to approximately 60 percent of crime-related losses at these businesses.

A-14 Employee Pilferage

a. Creating the Environment. The lack of initiative at the management/supervisory level **within** operational consumer outlets does little to prevent or reduce pilferage. Such shortcomings are identified as:

(1) Failure to present professional image:

❑ Lack of continuing interest, motivation, and direction.
❑ No alertness to internal control of pilferage.

(2) Failure to institute and implement methods of operational effectiveness and efficiency, such as:

- Clearly defined delegation of responsibility.
- Insistence on stringent accountability.
- Orientation and training programs for subordinate supervisors, current and new employees.

(3) Failure to emphasize and enforce established criteria for continual employment.

❑ Rules of conduct.
❑ Standards of job performance. **(Officially request appropriate action for employees guilty of criminal acts or infractions conducive to criminal acts.)**

(4) Inattentive job attitudes of subordinate supervisors.

(5) Inadequate personal checks of established accounting and inventory procedures.

> **Note:** Checks on both a regular and unannounced basis tend to control access to official stock records and to insure careful and organized storage or stocking of merchandise.

(6) Infrequent observation of employees' job performance.

(7) Failure to report misconduct, criminal or otherwise, to superiors and/or responsible law enforcement personnel in the activity.

(8) Failure to implement recommendations made during physical security inspections or crime prevention surveys.

b. Accomplishing the Act of Pilferage. The act may be accomplished by individual employees, more than one employee working as a team, or by employees and patrons in collusion. These actions can be greatly reduced by tightening supervision and security in the following areas:

(1) Merchandise display or dispensing areas.

- Detect unauthorized price reductions.
- prevent or make it difficult to alter price tags.
- Check procedures for declaring merchandise old, shopworn, damaged, or salvage.
- Provide more unpackaged items for personal consumption.
- Discourage careless waste of foods and other perishable items.

(2) Cash registers.

(a) Theft of cash is common:

- ❑ Direct from an unattended register.
- ❑ By rerunning register tapes at lower figures. (Preventable if reset key is maintained by the supervisor.)
- ❑ By clearing the register at a lower total figure than actual receipts for the operational period.
- ❑ By falsely reporting over-rings and refunds.

(b) Theft of merchandise is common to the following:

- ■ Under-rings
- ■ **Reuse of cash register tapes** occurs when employees fail to provide patrons with tapes or patrons allow employees to retain tapes (for theft or fail to recognize the crime prevention measure in asking for tapes). The tapes allow employees to package merchandise and remove it from premises.

(3) Removal of items from bags or containers by carry-out employees.

A-15 Patron Pilferage (Shoplifting)

This type pilferage is usually confined to sales areas and is committed by casual and systematic pilferers. **Items most frequently pilfered:**

- ■ Relatively small in size.
- ■ High degree of consumer desirability.
- ■ Easily carried in pocketbooks or secreted on the person.

a. Profiles of Shoplifters.

(1) Amateur adult shoplifters share these characteristics:

- Sudden temptation—impulse theft. Success in initial thefts, more temptation, stronger impulses, more thefts.
- Rarely a genuine need for the item. Generally has enough money to pay for item(s).
- Displays symptoms of nervousness and uneasiness.

(2) Juvenile shoplifters have the following traits:

- ❑ Act on a dare or "to belong."
- ❑ May be coached and/directed by an adult.

(3) Professional shoplifters share these characteristics:

- May be talkative, usually polite and deliberate.
- Continually looks for opportunities.
- Does not take many chances.
- Very capable of spotting security personnel.
- Steals for resale.
- Usually has "fences."
- Often steals "to order." May have a list describing the items to be pilfered.
- Employs innovative techniques.

(4) Kelptomaniacs:

- ❑ Take items without regard to value or use.
- ❑ Steal compulsively, often openly.
- ❑ Nervous and shy.

> **Note:** Genuine cases of kleptomania are rare.

(5) Narcotic addicts as shoplifters are described as follows:

❑ Desperate need for money and fear of imprisonment.
❑ Take long chances.
❑ Quickly take merchandise and exit premises.
❑ Steal usually at lowest physical and/or psychological ebb.
❑ **Dangerous if apprehension is attempted.**
❑ Habitually resists apprehension, **often violently.**
❑ **Only military police/security personnel should attempt apprehension,** not employees.

(6) Alcoholics and vagrants as shoplifters share these traits:

■ Usually steal because of need.
■ Often under the influence of liquor at the time of theft.
■ Usually, quickly take merchandise and exit.
■ Less likely to repeat regularly at a single location.

b. Environment for Shoplifting.

(1) Greatest pilferage occurs when employee coverage is low and/or when employees are untrained, inexperienced, or indifferent to the issue.

(2) Ineffective use of floor space aids shoplifters by creating congestion in the patron traffic flow.

(3) Allowing an emphasis on small rooms and/or partitioned areas causes congestion, which clusters, isolates, and/or partially hides displays.

c. Accomplishing the Act. This involves use of one or more of the following means to obtain items:

(1) Palming or placing an open hand on a small article, squeezing the muscles of the hand over the article to grasp it, and lifting the still open and apparently empty hand.

(2) Use of fitting rooms to put on tight or close fitting garments under clothing worn into the store.

(3) Trying on unpurchased hats, gloves, sweaters, jackets, and like item, then exiting the store—is a very common practice.

(4) Stepping around counters and removing items from unlocked showcases.

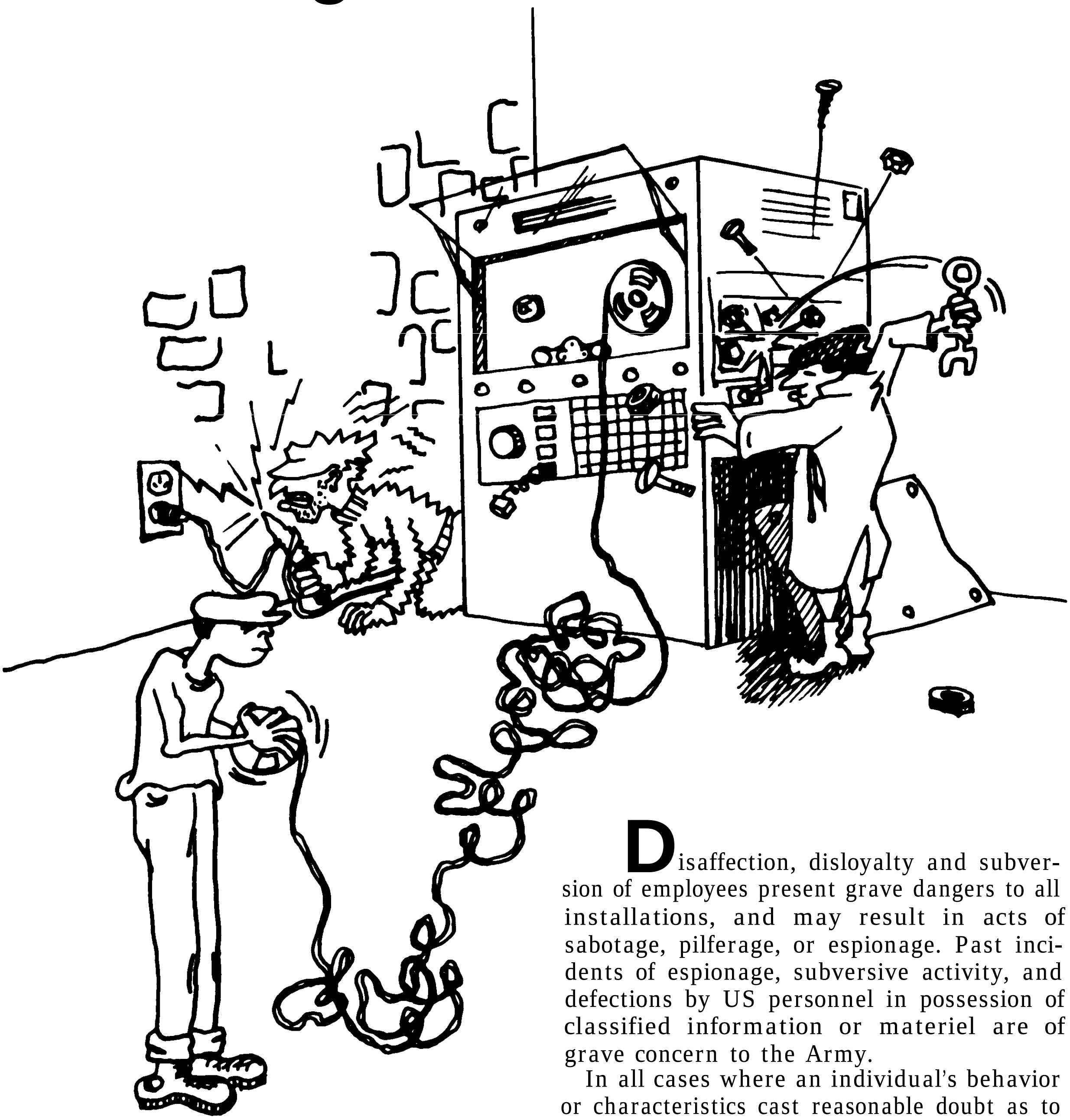
(5) Handling several items at once and replacing all except the item(s) pilfered.

(6) Use of accomplices to create a diversion of employee attention when secreting items on the person. Such items include:

- Clothing.
- Pocketbook and handbags.
- Umbrellas.
- Various items placed in packages or paper sacks containing merchandise paid for at other departments.

Appendix B

Sabotage



Disaffection, disloyalty and subversion of employees present grave dangers to all installations, and may result in acts of sabotage, pilferage, or espionage. Past incidents of espionage, subversive activity, and defections by US personnel in possession of classified information or materiel are of grave concern to the Army.

In all cases where an individual's behavior or characteristics cast reasonable doubt as to

his reliability or suitability, aggressive command action must be promptly taken to suspend his security clearance and thereby immediately withdraw access to classified information, materiel, or activities. Commanders and supervisors must administer this program so as to assure continued alertness for any indication of disqualifying conduct.

The primary purpose of this appendix is to expedite identification of persons with beliefs or traits of character dangerous to national security and their denial of appointment to, or removal from, positions of trust in which they could do significant harm to national interests.

B-1 The Sabotage Threat

Sabotage is defined in Federal law as any act that may injure, interfere with or obstruct the United States or any associate nation in preparing for or in carrying on war, or any act in willfully making, in a defective manner, war materiel or any tool used in making war materiel. It is the willful and malicious disruption of the normal processes and functions of the nation with respect to the national defense (chapter 645, Public Law 772, Aug 1948, 18 US Code 2153-2156).

a. Since Title 18 is a punitive law, the scope of sabotage which it defines is somewhat limited. Security personnel have a broader interest in this area, and should **expand this definition to include any act which maliciously destroys property or disrupts the operation or mission of an installation or facility for any reason whatever.** This includes vandalism, as defined in various dictionaries. Whether such vandalism could be chargeable as sabotage under the cited law is a matter for legal decision, and must be referred to the staff judge advocate.

b. The highly effective results which may be accomplished by the skillful employment of sabotage, and the known existence of certain groups available and willing to undertake such work, place this hazard high on the list of risks confronting the Army. In terms of trained manpower, equipment, and risk, a sabotage operation involves only negligible expenditure by the enemy; but the profit may be enormous if the target has been strategically selected.

c. The greatest danger of sabotage lies in concerted, simultaneous covert sabotage attempts against sensitive military installations or facilities, which, if successful, could seriously jeopardize military operations and could prevent tactical commanders from performing combat missions. **It is this threat of sabotage that requires sabotage alert procedures to be an important part of physical security plans.**

d. Sabotage as a diversion measure:

(1) Sabotage, particularly in the form of fire or minor explosions, may also be used as a diversion to permit pilferage, by drawing attention to the affected area and away from the object of the pilferage.

(2) This hazard exists particularly when security personnel are also responsible for firefighting and similar control operations.

B-2 Recognizing Sabotage

Recognition of an act of sabotage as such is often difficult, as the ultimate target may not be readily apparent and the act itself frequently destroys evidence of sabotage. To employ effective countermeasures against the threat of sabotage, it is necessary to understand some of the methods and targets of the saboteur.

B-3 Characteristics Of Saboteurs

a. May be highly trained professionals or rank amateurs.

b. May be computer programmers, laborers, machinists, flight engineers, foremen, or members of the management.

c. May be specially trained enemy agents assigned a specific mission or individual enemy sympathizers, or disaffected natives who act for their own personal reasons or interests.

d. May work alone or in groups. They may infiltrate military or industrial groups as legitimate members, or they may work from the outside.

e. May or may not have affiliation with foreign or military groups.

f. May be discontented employees.

g. Very vulnerable to subversive propaganda.

h. Maybe mentally ill.

i. Actions cannot be predicted or anticipated.

j. Acts on impulse.

B-4 Characteristics Of Enemy Special Agents

a. Directed, trained, supported, and supplied by a sabotage organization.

b. Coordinate efforts in an overall attempt to impede or disrupt industrial potential.

c. May lie dormant for years awaiting desired opportunity.

d. The motivation of an enemy special agent or an enemy sympathizer is obvious. The motivations of disaffected natives are much more complex. Correspondingly such agents are more difficult to detect, and individual motives may be as varied as the personality.

e. Agents may work for:

- Pay
- Hatred
- Revenge
- Sincere beliefs
- Settling real or imaginary grievances
- Blackmail purposes.

B-5 Sabotage Targets

In choosing their targets, saboteurs are influenced by two basic considerations analogous to those found in a tactical situation; namely, the objective, and how best to attain it. Is the destruction of the target to be sufficient in itself, or is it but a contribution to a larger plan? The ultimate in sabotage is complete and permanent destruction of the target. When this cannot be attained there may be many lesser targets, and enough of these strategically grouped may achieve comparable results.

B-6 Target Analysis

In analyzing a sabotage target, the saboteur considers the following factors:

a. The importance of the installation or facility from a technical or military standpoint. Will its complete or partial destruction hinder or breach the overall defense?

b. When complete destruction is not possible, what specific items of technical or military importance will have the most crippling effect on the mission of the installation? Examples of such items are:

(1) Rail yards and train equipment.

(2) Transformers at power stations.

(3) Dies in machine shops.

(4) Pumps at waterworks.

(5) Condensers at steam power plants.

(6) Fuel pipelines.

(7) Weapons and ammunition storage points.

(8) Airfields and airstrips and their facilities.

c. The capability of a target for self-destruction is always attractive to a saboteur. Heavy rotating machinery, such as turboelectric generators, can be ruined by a disturbance of the shaft alinement or by placing abrasives in the lubrication system. Other examples of self-destroying targets include ammunition and gasoline dumps, dams, and warehouses containing inflammable stocks.

B-7 Methods of Attack

The following specific targets are vulnerable to one or more methods of sabotage:

a. Natural Resources.

(1) Mines may be sabotaged by causing cave-ins or flooding of the shafts or tunnels.

(2) Forests may be destroyed by incendiaries; fruit trees maybe killed by an induced blight.

(3) Farm produce is vulnerable to parasites and various blights, and on a smaller scale by the diversion of water used for irrigation.

b. Army, Navy, Marine, and Air Force Installations or Facilities. Any action against an armed forces installation or facility, which disrupts or prevents full accomplishment of its mission, constitutes a potential threat. Sabotage actions intended to destruct ammunition or fuel supplies, and to disrupt communications, are common to all of the armed services. Other targets are peculiar to each service, such as drydocks and repair facilities to the Navy, and complex flight and navigation equipment to the Air Force. Headquarters buildings and billets located outside the installation or facility are specific targets of terrorists and insurgents, especially by bombing and arson.

c. Industry. Industry presents innumerable possibilities for explosive and mechanical sabotage, and is especially vulnerable to acts that will initiate a chain reaction. The following are examples of means by which sabotage can be committed in industrial processes:

(1) Drainage of oil or blocking of lubrication pipelines.

(2) Introduction of abrasives into machinery.

(3) Missetting or damaging process control instruments.

(4) Introduction of small tools or other pieces of metal into moving gears.

(5) Explosive charges placed to have a shattering effect when detonated.

d. Warehouses and Supply Depots. Materiel in storage is subject to ordinary explosive or incendiary sabotage. There is also an opportunity for delayed sabotage by the introduction of abrasives, contaminants, or adulterants into the items stockpiled. This latter type of sabotage will not normally be discovered until the materiel is put into use, and is difficult to detect or trace.

e. Transportation. The propelling machinery and cargoes of land, sea, and air transportation are subject to acts of sabotage similar to those mentioned in paragraph c above. In addition, rail transportation can be sabotaged by damaging switches, rails, roadbeds, and various structural adjuncts, such as bridges, tunnels, and shop facilities.

f. Materials Intransit. Supplies or equipment of any type intransit may be sabotaged, either by sabotaging the, means of transportation or by directly attacking the materials, or both. A bomb or arson device placed in the hold of a ship may damage or destroy both the cargo and the ship. A bomb or arson device used against a railroad tank car may destroy the car, its contents, and a portion of the rail line. The same applies to POL pipelines.

B-8 Sabotage Methods

There are many ways to commit sabotage, and new methods and devices are constantly being adopted.

a. A **major sabotage effort** may be undertaken **after thorough study** of the physical layout of the facility and its production processes by technical personnel fully qualified to select the most effective method to strike one or more of the most vulnerable parts of the facility.

b. Sabotage may, on the other hand, be **improvised by the saboteur,** relying solely upon his own knowledge of the facility and the materials available to him. The device or agent selected for sabotage may range from the crude or elementary to the ingenious or scientific.

c. The methods of sabotage may be classifed as follows:

❑ Fire
❑ Explosive devices
❑ Mechanical devices
❑ Chemical
❑ Psychological.

(1) Sabotage by Fire. The malicious use of fire is one of the oldest methods of sabotage. It is one of the most effective methods because it can result in destruction of the evidence as well as complete destruction of the objective.

(a) By using a timing device, the saboteur can have time to leave the area and establish an alibi, and it is entirely possible that the fire itself will leave minimum identifiable traces of its causes.

(b) Personnel assigned firefighting duties must be trained to recognize the various incendiary materials which may be used, and in the use of the appropriate extinguishing agent(s). Assistance in such training can be obtained from post engineers and fire departments.

(c) Incendiary materials include:

- Phosphorous
- Sodium
- Thermite
- Potassium

(2) Sabotage by Mechanical Devices. Mechanical delay devices are frequently used with dry cell electric batteries.

(a) The basic idea in these mechanisms can be well represented by the use of an ordinary pocket watch. By removing the minute hand, setting a small screw in the crystal to a depth that it will contact the hour hand but not the minute hand, and using this screw and the main stem as contact points to complete the electrical circuit, the watch becomes a timing delay mechanism with a 12-hour span (figure B-1). This same principle is employed in the majority of mechanical delay devices.

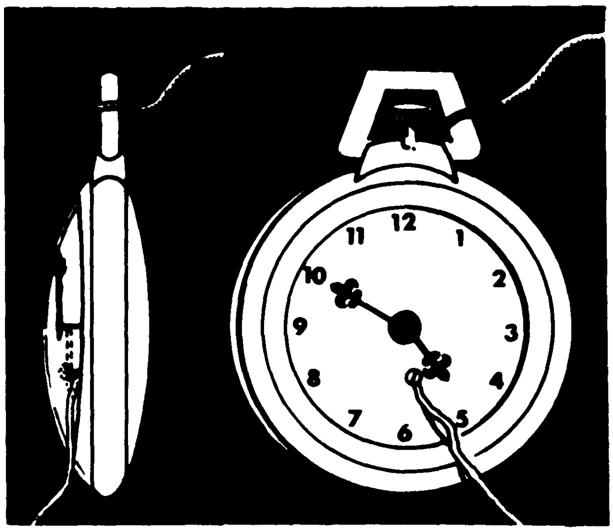


Figure B-1—Simple mechanical device.

(b) Other, and simpler delay devices can be devised, limited only by the ingenuity of the saboteur. For example, a rubber band may be used to hold the safety lever of a hand grenade in place. The pin is then pulled out, and the grenade is placed in a gasoline tank. The rubber band eventually rots, and an explosion and fire result. In a motor pool or refueling area, the widespread results can be disastrous:

(3) Sabotage by Explosives. The use of explosives achieves instantaneous, at least partial, destruction of the target, and the initial damage may be followed by a fire. The most probable targets are power and transportation facilities.

(a) Small quantities of explosives may trigger a chain reaction or destroy an extremely vital portion of an installation.

(b) One problem to the saboteur in explosive sabotage is the **difficulty of surreptitiously bringing explosives to the target.** For example, only approximately three pounds of an explosive can be concealed on a person. A saboteur may use any ingenious method to accomplish his mission.

(c) Explosives are readily available, and are used extensively in mining, agricultural, and some industrial operations. Also they are not difficult to produce, and the ingredients are readily procurable. These factors work to the advantage of the saboteur.

(4) Chemical agents may be easily introduced into installations by such means as air vents or heating systems. **Likely targets** for chemical agent sabotage are **installations employing highly skilled technicians.** Toxic chemical agents and incapacitating agents are highly effective and may cause employee productive efforts to be totally impaired.

(5) Psychological sabotage is most difficult to control or combat because it deals in intangibles and takes full advantage of normal human frailties. In its simplest form it is the implanting of a doubt or fear in the mind of an individual. It depends on natural rumor spreading for exaggeration and multiplication.

(a) Psychological sabotage may be employed effectively on a local scale to corrupt a unit or an installation. A definite distinction must be made, however, between manpower sabotage by psychological means, such as the instigation of strikes, slowdowns, and the like, and legitimate labor activities. Manpower sabotage of this nature is extremely difficult to detect. One disloyal employee engaged in psychological sabotage may influence others who will thereupon, believing in good faith that a labor grievance exists, engage in strikes and other activities resulting in loss of production.

(b) Another form of psychological sabotage is creation of panic through the

Common Explosives

Low Explosives	High Explosives
■ Black Powder	□ Nitroglycerin
■ Smokeless Powder	□ Dynamite
	□ Trinitrotoluene (TNT)
	□ Nitrostarch
	□ Composition C3 and C4

spreading of false, exaggerated, or distorted information or rumors. Panic has its basis in fear, and is usually the result of lack of knowledge of the truth or lack of confidence in leadership. In this type of sabotage, damaging rumors or surreptitiously distributed printed matter may be encountered by security forces who should be properly trained in countermeasures to combat this and other types of sabotage.

B-9 Sabotage Bombs

An explosive bomb itself is the unit of destruction and is not dependent upon outside aid as is an incendiary bomb; it is, therefore, normally larger than an incendiary bomb. However, the same ingenuity of disguise is applicable as in the case of an incendiary bomb.

a. Five sticks of dynamite taped together and equipped with a blasting cap would make an effective bomb, but upon sight would incite suspicion and concern. The same five sticks of dynamite stuffed in a suitcase with a dry cell battery and a clock-work delay device would be just as destructive, but would not attract attention.

b. A lump of plastic explosive coated with a mixture of shellac and coal dust would be unnoticed in a load of coal. The possible combinations of explosive, activator, delay device, and outside containers are many.

B-10 Bomb Handling

In any discussion of the handling, disarming, or disposal of sabotage bombs, it must be realized that the exterior appearance of a known or suspected bomb gives little or no indication of the explosive used or the manner of construction. Both of these key factors are largely dependent upon the availability of materials and the technical skill of the saboteur.

a. In view of the infinite varieties possible, it is obvious that no set procedure can be established for their handling. However, the primary consideration is the safety of life and property, and there are certain basic rules which must be followed.

b. Wherever the possibility of a sabotage bomb exists, there must be a **prearranged plan for coping with such an emergency** so that the following steps maybe earned out quickly and in many cases concurrently:

(1) Clear the area of all personnel, cordon the area, and establish a guard control around the danger zone.

(2) Send for technical help such as the explosive ordnance disposal unit, engineer personnel, or civilian police bomb squad.

(3) Immediately notify the security force headquarters.

(4) Shut off power, gas, and fuel lines leading into the danger area.

(5) Notify the fire department, medical service, MI and Federal Bureau of Investigation, as appropriate.

(6) Secure mattresses or sandbags for use as protective shields and barricades. Sandbags may also be used in confining and directing the force of an explosion.

(7) Remove flammable materials and small objects from the surrounding area. However, anything that might be connected with the bomb or might act as a trigger mechanism must not be touched.

(8) Arrange for the use of portable X-ray fluoroscopic equipment, which will be used by technical personnel only.

(9) See FM 19-5, chapter 12, and appendix D of this manual.

B-11 Countersabotage

Countermeasures against sabotage include, but are not limited to, the following:

a. Planning (chapter 1).

b. Risk analysis and evaluation (chapter 1).

c. Education (chapter 3).

d. Protective barriers (chapter 5).

e. Identification and movement control systems (chapter 4).

f. Searches of incoming vehicles (chapter 4).

g. Restricted areas (chapters 4 and 5).

h. Safeguarding classified information.

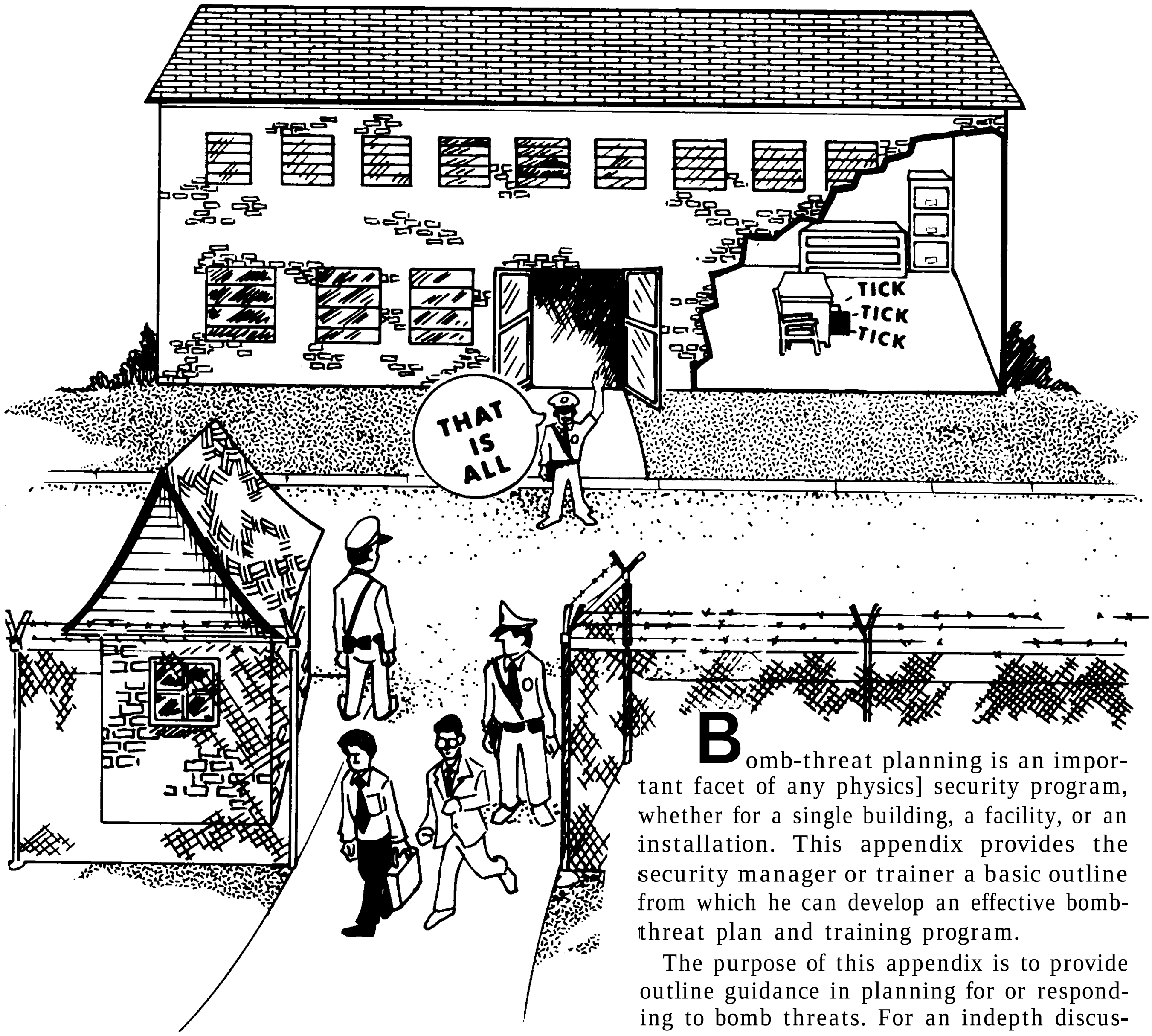
i. Investigation of securit y breaches (chapter 9).

j. Physical security surveys and inspections (chapter 17).

k. Of utmost importance is the building and maintaining of employee morale, informing employees of threatened dangers, how they may be recognized and what protective measures are available.

Appendix D

Bomb Threats



Bomb-threat planning is an important facet of any physics] security program, whether for a single building, a facility, or an installation. This appendix provides the security manager or trainer a basic outline from which he can develop an effective bomb-threat plan and training program.

The purpose of this appendix is to provide outline guidance in planning for or responding to bomb threats. For an indepth discussion, review TC 19-5.

153-846 O - 94 - 13

D-1 Definitions

a. A **bomb** is a device capable of producing damage to material and injury or death to personnel when detonated or ignited. Bombs are classified as explosive or incendiary. An explosive bomb causes damage by fragmentation, heat, and blast wave. The heat produced often causes a secondary incendiary effect. An incendiary bomb generates fire-producing heat without substantial explosion when ignited.

Bombing occurs when an explosive bomb detonates, or an incendiary bomb ignites.

b. A **bomb threat is** a message delivered by any means and the message mayor may not:

■ Specify location of the bomb.
■ Include the time for detonation/ignition.
■ Contain an ultimatum related to the detonation/ignitor or concealment of the bomb.

c. A **bomb incident** involves any occurrence concerning the detonation/ignition of a bomb, the discovery of a bomb, or execution of a bomb threat.

D-2 Countermeasures

Measures taken to minimize the production and placement of bombs to include reducing the disruptive effects are as outlined:

a. Preplanning considerations (figure D-1).

(1) Preplanning is an essential prerequisite for developing a workable bomb threat plan. In the preplanning phase, provision must be made for:

● Communication channels
● Support organizations
 ● Primary
 ● Alternate.

(2) Communication equipment. Do not operate radio transmitters in the vicinity of the device. They could detonate it. The following elements should have communications capability:

■ Emergency operations center
■ Facility/area inspections
■ Reporting system
■ Search teams
■ Security teams.

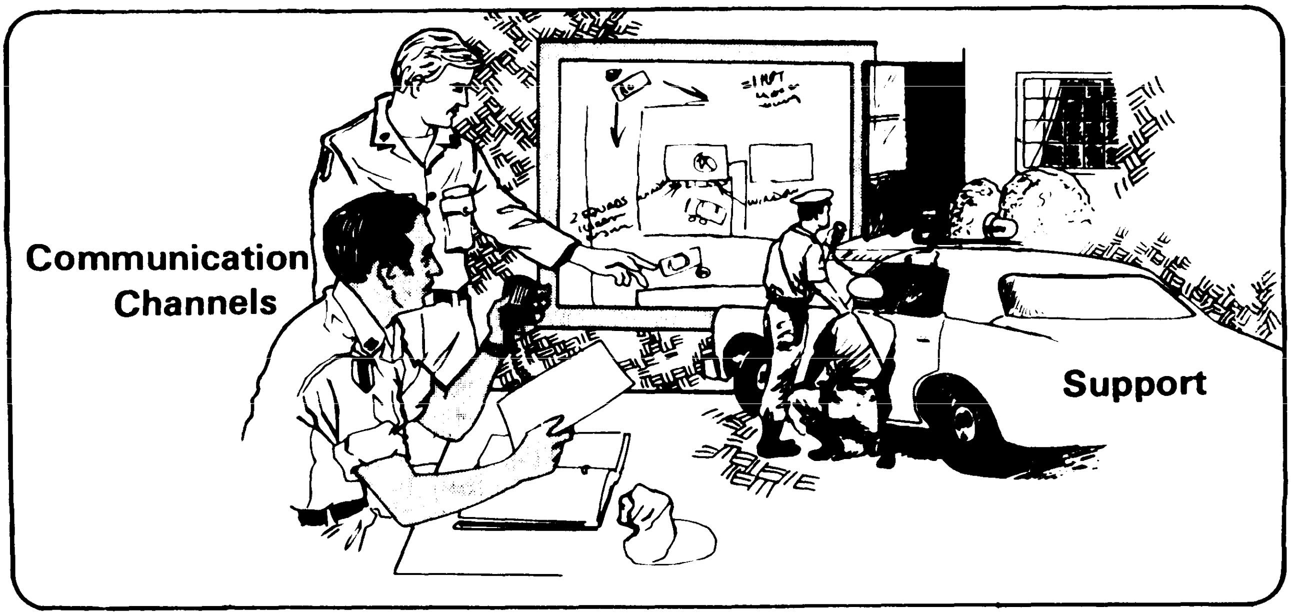


Figure D-1—Effective bomb threat reaction must include communication and support.

b. Prepare the bomb threat plan. Any effective plan must address at least the following considerations

☐ Control of the operation.
☐ Evacuation.
☐ Search.
☐ Finding the bomb or suspected bomb.
☐ Disposal—EOD.
☐ Detonation and damage control-Barricade material around the device to guide device fragments upward.
☐ Control of publicity.
☐ Erection of barriers.
☐ Fire and medical service standby.
☐ Disconnection of utilities.
☐ Removal of flammables/expolsives.
☐ After action report.

c. Evaluate the threat.

d. Activate the plan.

D-3 How To

A bomb threat may be received by any of the following:

- Telephone message
- Suspicious package through the mail
- Written message through the mail.

a. Search Techniques (figure D-2). The choice of search techniques will depend on whether the threat is overt or covert. The following decisions must be made before the proper techniques can be applied:

☐ Conducted prior, after, or without evacuation
☐ Conducted by supervisors, occupants, or a special team
☐ Percent of building to be searched
☐ If a search team is used, it should be divided as follows:

Decisions for Bomb Threat Search

When do you search?
- Before evacuation
- After evacuation
- Without evacuation

Who does the searching?
- Occupants
- Supervisors
- Special team

How is search conducted?
- Area outside of building
- Public areas
- Detailed search of building

What equipment is needed and available?

Figure D-2—Search technique decisions to be made.

- ■ Outside search 25 percent.
- ■ Public areas 25 percent.
- ■ Detailed building search 50 percent.

b. Equipment

- Specialized.
- Available.

c. Evacuation Procedures **(threat received** and **bomb found).**

(1) Predesignated routes of evacuation.

(2) Priorities for people removal.

(3) Predesignated guides.

(4) Other considerations:

- ❑ Authority to order evacuation.
- ❑ Decision to permit reentry into building.
- ❑ The signal to evacuate.
- ❑ Who will be the evacuation team.
- ❑ What are the evacuation procedures.
- ❑ Destination of evacuation occupants.
- ❑ Responsibilities of the occupants during evacuation.

d. Telephone Procedures Bomb Threat Checklist.

Instructions: Be calm. Be courteous. Listen, do not interrupt the caller. Notify supervisor/security officer by prearranged signal while caller is on line.

Name of Operator ______________________ **Time** __________ **Date** __________

Caller's Identity

Sex: ☐ Male ☐ Female ☐ Adult ☐ Juvenile Approximate Age: Years __________

Origin of Call

☐ Local ☐ Booth ☐ Internal (From within bldg?)
☐ Long Distance
If internal leave line open for tracing the call.

Voice Characteristics

☐ Loud ☐ Soft
☐ High Pitch ☐ Deep
☐ Raspy ☐ Pleasant
☐ Intoxicated ☐ Other ____

Speech

☐ Fast ☐ Slow
☐ Distinct ☐ Distorted
☐ Stutter ☐ Nasal
☐ Slurred ☐ Lisp
☐ Other ____

Language

☐ Excellent ☐ Good
☐ Fair ☐ Poor
☐ Foul ☐ Other ____

Accent

☐ Local
☐ Not Local
Region ____
☐ Foreign
Race ____

Manner

☐ Calm ☐ Angry
☐ Rational ☐ Irrational
☐ Coherent ☐ Incoherent
☐ Deliberate ☐ Emotional
☐ Righteous ☐ Laughing

Background Noises

☐ Factory Machines ☐ Trains
☐ Bedlam ☐ Animals
☐ Music ☐ Quiet
☐ Office Machines ☐ Voices
☐ Mixed ☐ Airplanes
☐ Street Traffic ☐ Party Atmosphere

Bomb Facts

Pretend difficulty with your hearing. Keep caller talking.

If caller seems agreeable to further conversation, ask questions like:

When will it go off? Certain Hour—Time Remaining— What kind of bomb?—Where are you now? How do you know so much about the bomb?—What is your name and address?

If building is occupied, inform caller that detonation could cause injury or death.
Did caller appear familiar with plant or building by his description of the bomb location?

Write out the message in its entirety and any other comments on a separate sheet of paper and attach to this checklist.

Action To Take Immediately After Call

Notify your supervisor/security officer as instructed. Talk to no one other than as instructed by your supervisor/security officer.

Appendix E

Countering Terrorism



Incidents of terrorism take place almost daily. Therefore, it is essential that security personnel know what to expect from terrorists and something of their beliefs and goals. This appendix addresses the following aspects of terrorism:

- ❑ History of violence
- ❑ The threat

- ❑ Target selection
- ❑ News media
- ❑ Weapons
- ❑ Typical operations
- ❑ Methods
- ❑ Jurisdiction
- ❑ Reporting incidents
- ❑ Installation vulnerability
- ❑ Countermeasures.

E-1 History of Violence

a. Violence dates back thousands of years. Torture was prevalent then and persisted into the 18th and 19th centuries. The 20th century introduced various forms of chemical and psychological torture.

b. Terrorism, historically, is most closely related and referenced to the reign of terror of the French Revolution in 1793. This was the first time an attempt was made to create an organization outside of a governmental body, whose philosophy was to systematically murder and set a rule of lawlessness based upon a political belief.

c. The terrorist threat has encompassed all areas of government, business and community life—international, national, and local. Terrorists have acted to spread fear for the following reasons:

(1) Retaliation-for a variety of political and/or organizational reasons.

(2) Destruction of Property-a message warning, or sign of things to come.

(3) Taking of hostages as bargaining tools for various goals.

d. The use of terror has always been:

(1) A means of coercion.

(2) A well planned campaign. (It still is.)

(3) The threat that further violence is possible/probable.

E-2 Target Selection Criteria

a. For maximum shock effect.

b. An environment that presents a low risk to the assault team, such as isolated situations and sites.

c. High risk environments to demonstrate potential and ability, such as:

(1) Communication/operational nerve centers.

(2) Heavily populated living areas and/or establishments.

d. To gain international attention.

e. Assault a target because of the high dollar placed upon it.

f. For maximum disruption of a facility's operation.

E-3 News Media

The final result of all terrorist acts is that they receive widespread news media exposure. Results of such exposure must be considered in view of the following:

a. In hostage situations, the hostage has been known to identify with his captors. This association increases the difficulty of the situation.

b. Increase of publicity of an incident may increase sympathy for a particular cause.

E-4 Terrorist Weapons

a. The most common weapons of terrorists include:

(1) Handguns

(2) Automatic weapons

(3) Explosive devices

(4) Other sophisticated weapons.

b. Sale and smuggling of guns has forced increased security and enforcement measures by Federal agencies. It is estimated that there are some 40 million handguns in the possession of citizens in the United States. This does not include automatic weapons, explosive devices and rocket firepower.

c. Major concern and priority is to be given to installations with chemical and nuclear material. These sensitive installations must receive maximum security.

d. The handheld automatic weapon is a favorite of terrorist groups because of its availability, size, weight, ease of concealment, high rate of fire and psychological impact on lightly armed security forces or unarmed civilians.

E-5 What to Expect

Members of terrorist organizations usually meet these standards:

■ Well disciplined for violence.

■ Attacks are well planned.

■ Members are well armed and trained.

■ Expertly executed.

■ Reconnaissance conducted by persons other than strike force.

■ Terrorist assault and/or negotiation team has a designated leader.

■ Use available rapid transportation.

■ Terrorism techniques embrace:

- Subversion
- Penetration
- Indoctrination
- Direct assault
- Skyjacking
- Kidnapping
- Sabotage.

E-6 Methods of Operation

a. Robbery of needed equipment and supplies is an indication of possible terrorist activity, such as theft of ammunition, weapons, communications equipment, large amounts of paper, or copying machines to produce propaganda.

b. Attack selected persons or property to cause confusion, disorder or to force nations to confront one another.

c. Blackmail is an intelligence or Federal investigation matter. A DOD member maybe blackmailed into providing information about the installation.

d. Kidnapping a family member of a high ranking or influential officer of DOD as a hostage for ransom or other demand (figure E-1, page 304).

e. Arson of government property as a gesture of their ability.

f. Bombing of specific or indiscriminate targets to convey a message and display their serious intent on an issue.

g. Shootouts (ambushes) of guards to



Figure E-1—Family members are susceptible to kidnapping.

gain access to a restricted area. Critical areas of security demand reaction teams.

h. Hijacking of aircraft and trains.

E-7 Jurisdiction

Considerations must include the following on jurisdiction when planning and determining counterterrorism reactions:

a. Whether jurisdiction is concurrent or exclusive.

b. Proximity to installation borders.

c. Operational, investigative responsibility (Department of Justice, FBI).

d. Military abroad (Department of State).

e. Military forces command and operational control.

E-8 Reporting Incidents

a. Any terrorist incident must be reported immediately to security supervisors, operational alert centers, jurisdictional agencies, police response forces, and adjacent installations.

b. Security supervisory personnel should be familiar with command relationships during counterterrorism operations. Memorandums of understanding should be prepared and mutually signed concerning when and how FBI/military authorities interact during incidents. Also, how Status of Forces Agreements (SOFAS) apply in host countries when incidents occur on military installations. As a minimum, memorandums of understanding should include:

- Command-relationships and jurisdiction
- Sharing of information
- Control of military operations
- Organization-composition of joint forces
- Negotiating tactics
- Use of equipment
- Use of force measures
- Liaison with media and public officials.

E-9 Counterterrorism Actions

a. Each terrorist incident is categorized in three phases—initial response, negotiation, and assault.

(1) Initial response phase is the period during which military and security personnel become aware of a terrorist committed act and prepare to counter the act through peaceful persuasion or military force.

(a) Terrorists seize buildings and take hostages. The nearest military police or security patrol arrives on the scene to estimate the situation. Military police/security patrol report incident to the military police/guard operations desk.

(b) In CONUS, the following agencies are alerted:

- ❑ MP duty officer
- ❑ Provost marshal
- ❑ Installation headquarters
- ❑ Installation operations center
- ❑ CID
- ❑ MI

(c) The installation duty officer at the operations center notifies installation commander who informs:

- **FBI**
- Next Army operations center, DA, who alerts the next higher command (see figure E-2, next page).

(d) OCOPOS, installation headquarters operation centers contact the major command (USAREUR, Eighth Army, etc.). Alert notifications are cited in AR 190-40 (see figure E-3, page 307).

(e) Step-by-step:

- Initial on-scene commander with military and/or security police personnel sustains contact with terrorists and in accordance with doctrine and preestablished procedures, and attempts to ascertain a precise estimate of the situation.
- Provost marshal, or designated representative, arrives on scene at nearby location to establish forward command post, assuming forward operational control as commander. The initial, now former, commander remains at the command post to provide information and assistance.
- Security and reconnaissance personnel of the predesignated reaction force arrive on scene and establish physical security cordon of the area. They determine best access to and egress from the terrorist target (building with terrorists/hostages).
- Tactical elements or predesignated reaction force moves to assembly area beyond sight and hearing of terrorists and prepares for possible assault operations.
- Forward command post establishes communications with installation emergency operations center (IEOC).
- Installation commander arrives at IEOC to command counterterror operations, first obtaining an estimate of the situation from the provost marshal.

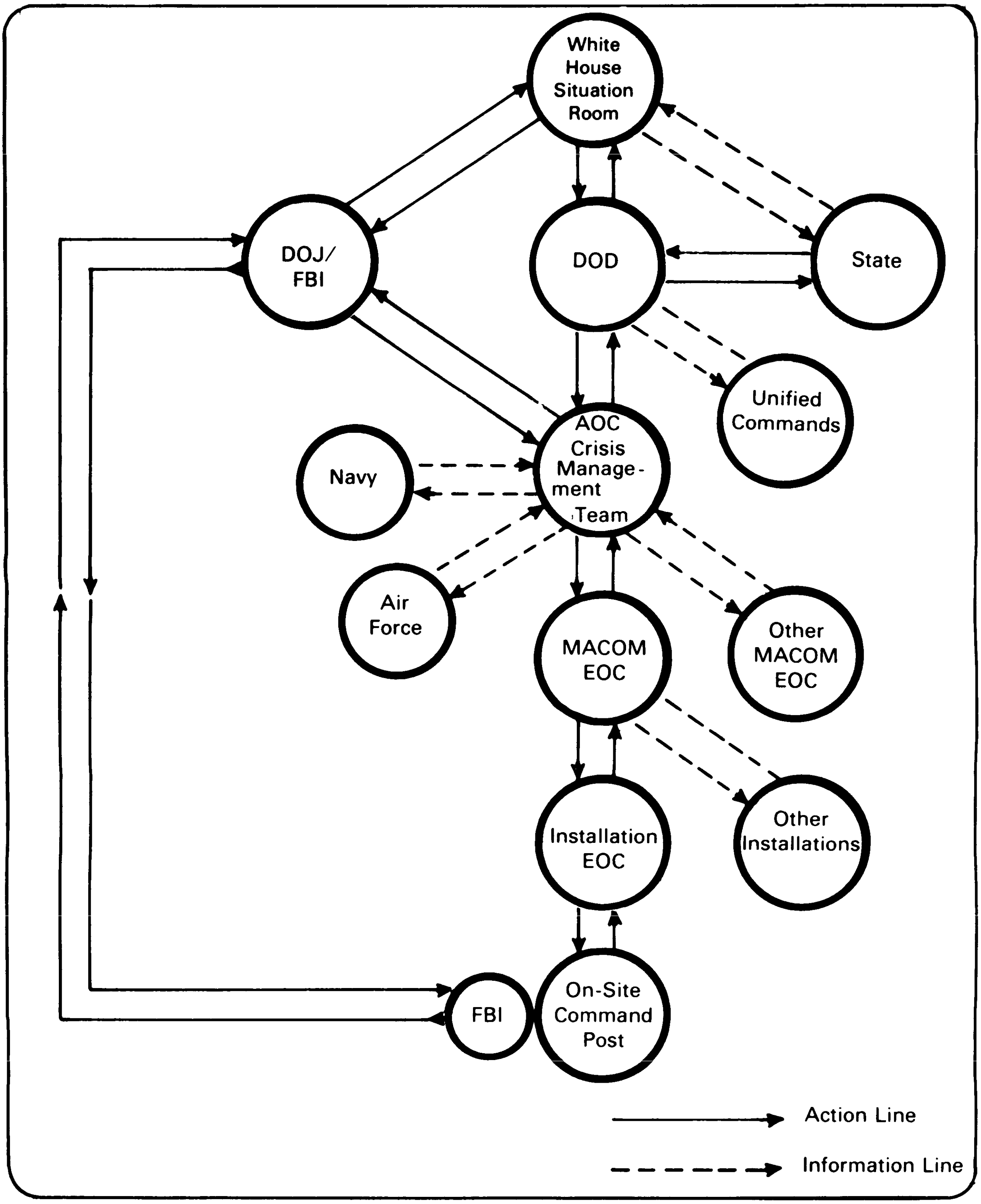


Figure E-2—CONUS Terrorist Alert Notification Process. This flowchart outlines notification channels and depicts interface with all areas of the government.

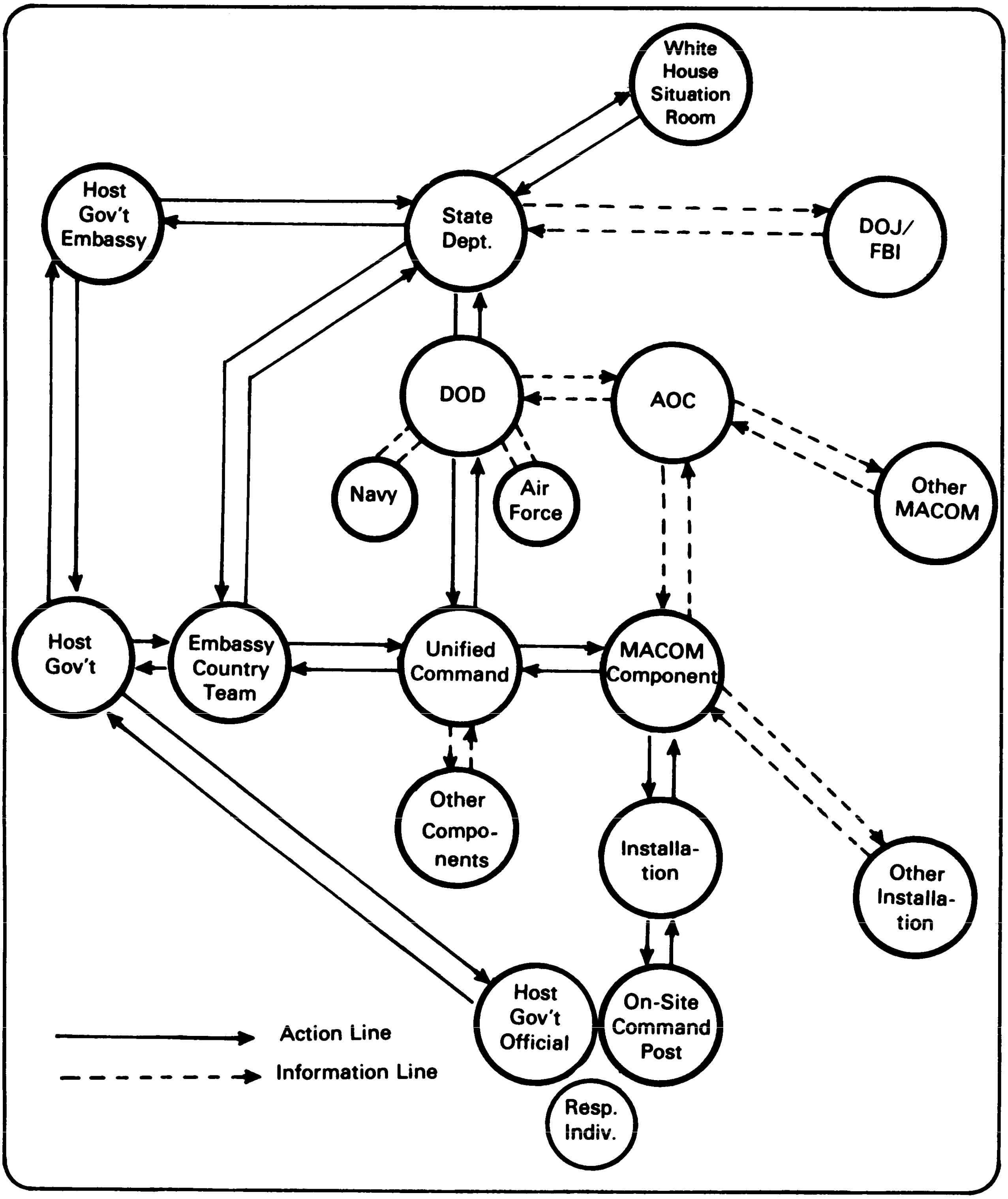


Figure E-3—OCONUS Terrorist Alert Notification Process.

- The provost marshal sustains contact with terrorists and determines:
  - The number of hostages, who they are, and their condition.
  - Precise interpretation of terrorist demands.
  - Number of terrorists, type of terrorist group(s), position of terrorists in the building, and movement patterns of both terrorists and hostages.
  - Name(s) of terrorists, especially the leaders.
  - Terrorist behavior characteristics (such as nervousness, tense, easily excitable, or unemotional).
  - Terrorist weapons, explosives, equipment.
  - Best access and egress to and from building (from reports by elements of the reaction force).
  - Tactical military options for use by tactical elements.
  - If available resources will support planned tactical military operations.
  - Begins formal negotiations with terrorists (NOTE: Terrorists may reject the assigned negotiator and request to negotiate only with installation commander or other official party.) Report results of all above to IEOC.
- Senior FBI official arrives at IEOC and receives briefing on situation from installation commander or provost marshal and assumes responsibility along with the installation commander as director of operations.

(2) Negotiation phase.

(a) Negotiating team, or negotiator, contacts the terrorists and buys as much time as possible from terrorists for the consideration of their demands.
(b) IEOC forwards clarification of demands to AOC/DA and awaits guidance on how the US Government will react. OCONUS reports to OPNS center, major command.
(c) Forward command post forwards to IEOC recommended tactical military options with estimated risk factors.
(d) IEOC analyzes tactical military options and determines best security option, then alerts forward command post of the option selected.
(e) Forward command post alerts support elements (such as medical, transportation, etc.) to embark on support mission.
(f) Forward command post alerts the leader of the tactical element and provides this individual with the military option plan although **permission to conduct such a plan is yet to be granted.**
(g) The option may be to conduct assaults to free hostages and take prisoners.
(h) Leader of tactical element returns to rear assembly area and briefs element to conduct the plan. Element obtains additional equipment, if needed, and undergoes full preparation, rehearsing actions repeatedly.
(i) FBI official and/or installation commander (US, i.e., on command prerogative) may move to forward command post. However, it should be noted that the appearance of additional authority may be viewed by terrorists as an indication of impending final action.
(j) AOC/DA forwards to IEOC a decision on use or nonuse of tactical military option. IEOC reports decision to forward command post (FCP) commander of the tactical element. If a decision is made to conduct tactical military operation(s), the third phase is initiated.

(3) Assault phase.

(a) Tactical element completes rehearsals, regroups at assembly area, establishes mobile command post, and informs forward command post when ready to embark on military operation.
(b) On order, tactical element moves as covertly as possible from assembly area to its objective.

b. Control is the essential element during

Evaluation of Situational Control/Counterterror

(Hostage Incident)

Phase	Exercising Direct Tactical Control	Exercising Indirect Tactical Control	Exercising Overall Strategic Decision-Making Control	Exercising Overall Policy Effects Control
Initial Response Phase	First authority on scene (MP)	Installation duty officer	Installation duty officer	
	Comdr, fwd CP (Provost marshal)	Comdr, IEOC (instal Comdr, or early-on a designated senior representative	Comdr, IEOC (as left of this column)	
Negotiation Phase	Comdr, fwd CP (Provost marshal) negotiator	Comdr, IEOC (Instal Comdr)	FBI official (and installation Comdr)	HQDA (AOC); or, as OCONUS situations, major command or US Dept State (embassy)
Assault Phase	Comdr, fwd CP Comdr, tactical element	IEOC (Instal Comdr)	FBI official	Same as above.

Figure E-4—Outline of control for hostage incident.

any of the three phases. The outcome of a terrorist event depends on counterterrorist situational control; therefore, command and control links must contain limitations imposed upon them by policy direction.

(1) Military and security poIice duties and responsibilities must be clearly established.
(2) Installation and unit contingency plans/SOP must be developed.
(3) Security personnel must be schooled and/or trained to react to a terrorist situation.

E-10 Vulnerability

a. To determine the vulnerability of any given installation, ten major factors are considered:

(1) Installation characteristics and sensitivity— personnel/mission. There are four subfactors.

(a) Consider personnel as hostage candidates. General officers and foreign personnel assigned to the installation.
(b) Sensitivity of the installation mission. Maximum consideration to nuclear or chemical storage sites.
(c) Consider open post versus closed post.
(d) The installation considered a symbol of national significance.

(2) Law enforcement resources-available personnel. Three categories to consider:

(a) Military
(b) Federal
(c) Local.

The law enforcement resource is responsible for law and order, and should be a priority when analyzing for safety and control. The military is immediately available and under direct control of the installation commander. FBI and local authorities are considered supplements to the military resources because of response time. Another important aspect is the number of MPs on duty or available within the required response time.

(3) Distance from population centers— miles/time. Experts on terrorism say that heavily populated urban areas usually provide these advantages to terrorists:

(a) Concealment of supplies and equipment.
(b) Safe houses are more readily available.
(c) More of a tendency for popular support.
(d) More freedom of movement.

On the other hand, low density population areas have the following characteristics:

(e) Strangers are noticed.

(f) Local law enforcement personnel tend to be close to day-to-day activities.

(4) Size of installation— area population.

(a) The larger the installation population the larger number of potential targets created due to increased requirements for arms, ammunition, banks, schools, clubs, etc.
(b) With increased population, the popularity for infiltration and support within is increased.

(5) Routes for access and egress— method of transportation. There are generally three major means of approaching and leaving a military installation-aircraft, vehicle, and boat. Because of the capabilities of a helicopter, all military installations are considered equally vulnerable. The number of roads and their quality should be considered. Only major waterways or large bodies of water should be viewed as transportation routes.

(6) Area social environment— social. Some geographical areas of the United States either have a history of, or a tendency for, unrest and dissident elements.

(7) Proximity to borders— jurisdiction. This factor of vulnerability takes into consideration the desirability of preparing for a terrorist attack in a foreign country and for escape after the act.

(8) Distance from other US military installation— support. Major governing factor is response time. If a local agreement for military support exists with a non-US military installation, the supporting force must be periodically exercised for an efficient cooperative response.

(9) Terrain. The terrain adjacent to the installation is another condition to be considered in overall installation vulnerability. Some types of terrain are built-up areas which present advantages to planning and executing a successful terrorist act or incident. (See TC 7-1, chapter 3, Cover, Concealment, Camouflage, and Target Acquisition.)

(10) Communications with next higher echelon.

(a) A significant influence is if terrorists have knowledge of the effectiveness of the installation communication system.

(b) Consider communications and the influence it may have on the outcome of a terrorist act.

(c) The more prolonged the act (such as hostage), the more influence communications can have in providing advice and assistance in coping with the situation. On the other hand, a bombing is a sudden event and the communications then serve primarily as a means of reporting.

(d) Both land and line telephone and radio must be evaluated. Land line telephone is more secure and reliable than radio because the radio is more subject to interruption either by terrorist act, by accident, or jamming.

(e) Interpersonal communication, your ability to perform your command of required security measures which will aid the safety of the installation, is a key factor.

b. Included with these ten factors are two aspects which are the results of actions taken by the installation commander. These two factors are **area social environment and law enforcement resources.**

c. The area social environment can be reduced to zero if the installation command and/or provost marshal is an active participant, on a regular basis, in meetings or councils with other area law enforcement agencies.

d. With the restriction imposed on Federal authorities in collection of domestic intelligence, close contact with state and local authorities provides the most effective means for staying current on the social environment surrounding the installation.

e. The assessed vulnerability value of the law enforcement factor can be reduced if military law enforcement assets have certain capabilities. These can be unique equipment or training:

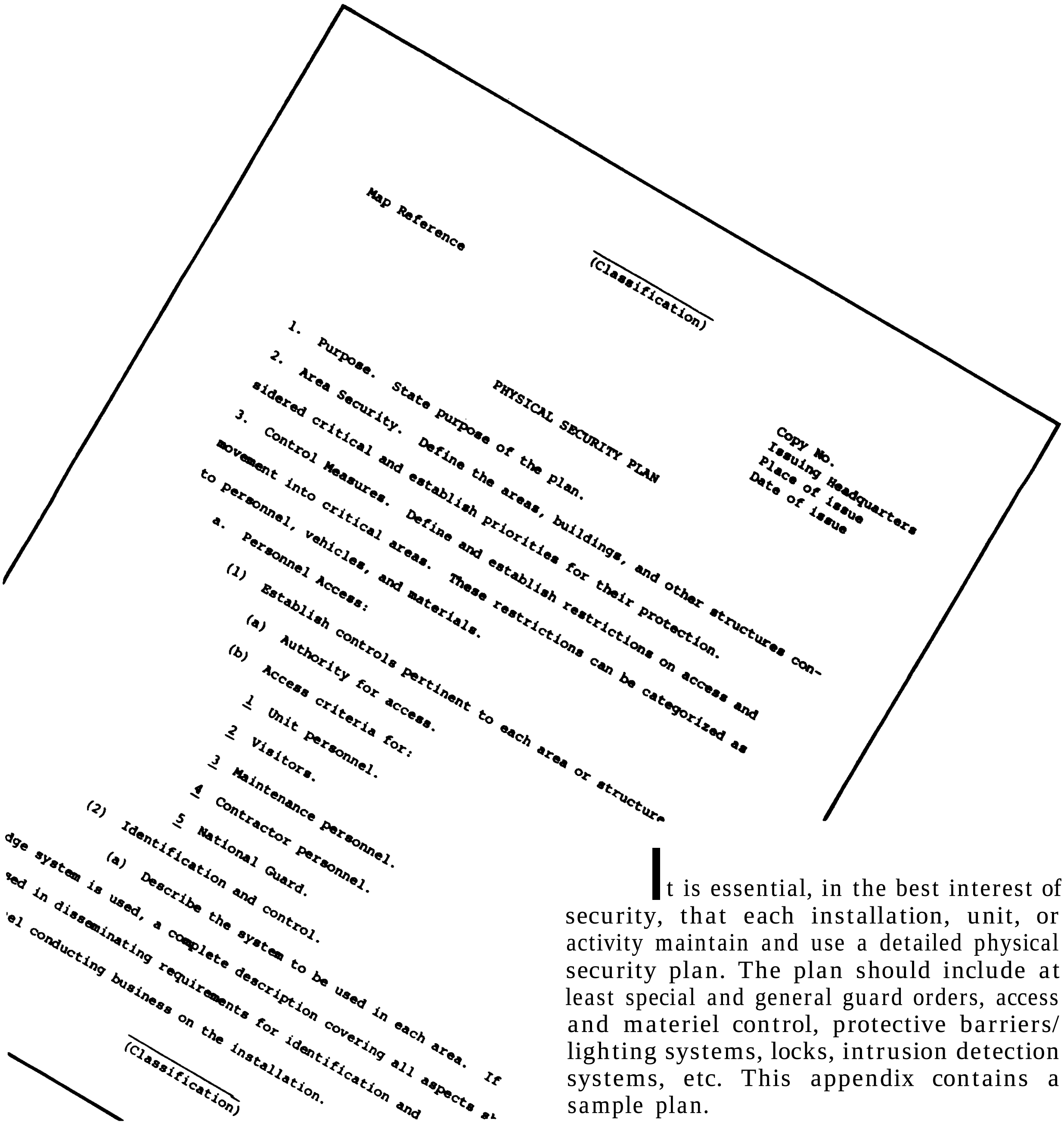
(1) Equipment, armored car, aircraft, special firearms and suppression devices.

(2) Unique training (such as sniper, special reaction team, negotiating team) gives additional capabilities to law enforcement personnel.

f. AR 190-13, The Army Physical Security Program, provides guidance as well as a formal system for surveys and inspections to test vulnerability of an installation.

Appendix F

Physical Security Plan



Map Reference

(Classification)

Copy No.
Issuing Headquarters
Place of issue
Date of issue

PHYSICAL SECURITY PLAN

1. Purpose. State purpose of the plan.

2. Area Security. Define the areas, buildings, and other structures considered critical and establish priorities for their protection.

3. Control Measures. Define and establish restrictions on access and movement into critical areas. These restrictions can be categorized as to personnel, vehicles, and materials.

a. Personnel Access:

(1) Establish controls pertinent to each area or structure

(a) Authority for access.

(b) Access criteria for:

1 Unit Personnel.

2 Visitors.

3 Maintenance Personnel.

4 Contractor Personnel.

5 National Guard.

(2) Identification and control.

(a) Describe the system to be used in each area. If

dge system is used, a complete description covering all aspects

ed in disseminating requirements for identification and

el conducting business on the installation.

(Classification)

It is essential, in the best interest of security, that each installation, unit, or activity maintain and use a detailed physical security plan. The plan should include at least special and general guard orders, access and materiel control, protective barriers/ lighting systems, locks, intrusion detection systems, etc. This appendix contains a sample plan.

(Classification)

Map Reference

Copy No.
Issuing Headquarters
Place of issue
Date of issue

PHYSICAL SECURITY PLAN

1. Purpose. State purpose of the plan.

2. Area Security. Define the areas, buildings, and other structures considered critical and establish priorities for their protection.

3. Control Measures. Define and establish restrictions on access and movement into critical areas. These restrictions can be categorized as to personnel, vehicles, and materials.

a. Personnel Access:

(1) Establish controls pertinent to each area or structure.

(a) Authority for access.

(b) Access criteria for:

1 Unit personnel.

2 Visitors.

3 Maintenance personnel.

4 Contractor personnel.

5 National Guard.

(2) Identification and control.

(a) Describe the system to be used in each area. If a badge system is used, a complete description covering all aspects should be used in disseminating requirements for identification and control of personnel conducting business on the installation.

 (Classification)

(b) Application of the system.

1 Unit personnel.

2 Visitors to restricted areas.

3 Visitors to administrative areas.

4 Vendors, tradesmen, etc.

5 Contractor personnel.

6 Maintenance or support personnel.

b. Material Control.

(1) Incoming.

(a) Requirements for admission of material and supplies.

(b) Search and inspection of material for possible sabotage hazards.

(c) Special controls on delivery of supplies and/or personnel shipments in restricted areas.

(2) Outgoing.

(a) Documentation required.

(b) Controls, as outlined in (1)(a), (b), and (c) above.

(c) Classified shipments NOT involving nuclear/chemical material.

(3) Nuclear/chemical material.

(a) Controls on movement of warheads/chemicals on the installation.

(b) Controls on shipments or movement of training warheads/chemicals.

(c) Controls on pickup or delivery of warheads/chemicals outside the installation.

c. Vehicle Control

(1) Policy on search of military and privately owned vehicles.

(2) Parking regulations.

(3) Controls for entrance into restricted and administrative areas.

(a) Privately owned vehicles.

(b) Military vehicles.

(c) Emergency vehicles.

d. Vehicle Registration.

4. Aids to Security. Indicate the manner in which the following listed aids to security will be implemented on the installation.

a. Protective barriers.

(1) Definition.

(2) Clear zones.

(a) Criteria.

(b) Maintenance.

(3) Signs.

(a) Types.

(b) Posting.

(4) Gates.

(a) Hours of operation.

(b) Security requirements.

(c) Lock security.

b. Protective Lighting System.

(1) Use and control.

(2) Inspection.

(3) Action to be taken in the event of commercial power failure.

(4) Action to be taken in the event of a failure of alternate source of power.

(5) Emergency lighting systems.

(a) Stationary.

(b) Portable.

c. Intrusion Detection Systems.

(1) Security classification.

(2) Inspection.

(3) Use and monitoring.

(4) Action to be taken in event of "Alarm" conditions.

(5) Maintenance.

(6) Alarm logs or registers.

(7) Sensitivity settings.

(8) Fail-safe and tamper-proof provisions.

(9) Monitor panel location.

d. Communications.

(1) Locations.

(2) Use.

(3) Tests.

(4) Authentication.

5. Security Forces. Include general instructions that would apply to all security force personnel (fixed and mobile). Detailed instructions such as Special Orders and SOP should be attached as annexes.

a. Composition and organization.

b. Tour of duty.

c. Essential posts and routes.

d. Weapons and equipment.

e. Training.

f. Use of sentry/patrol dogs.

g. Method of challenging with sign and countersign.

h. Alert force.

(1) Composition.

(2) Mission.

(3) Weapons and equipment.

(4) Location.

(5) Deployment concept.

6. Contingency Plans. Indicate required actions in response to various emergency situations. Detailed plans such as counterterrorism, bomb threats, hostage negotiation, disaster, fire, etc., should be attached as annexes.

a. Individual actions.

b. Alert force actions.

c. Security force actions.

7. Use of Air Surveillance.

8. Coordinating Instructions. Indicate matters which require coordination with other military and civil agencies.

a. Integration with plans of host or nearby military installations.

b. Liaison and coordination.

(1) Local civil authorities.

(2) Federal agencies.

(3) Military organizations.

/s/____________________________
Commander

Annexes:

A - Intelligence

B - Installation Security Status Map

C - Contingency Plans

D - Special Instructions to Security Officers/Managers and Officers of the Day

E - Commander of Relief Instructions

F - Sergeant of the Guard Instructions

G - Special Orders for Guard Posts

Appendix G

Contract Guards



This appendix contains a sample contract with appropriate special and general orders for security forces (in addition to those discussed in chapter 9). Contract guards are an inherent part of overall installation security forces. When considering the use of or the actual employment of contract guards, the area addressed in this appendix should apply. Contract guards are usually used when it is more feasible in terms of manpower resources and criticality y of the mission. A contract is essential when the Government provides the property and services to a contractor or when the Government maintains possession of the property and employs contract personnel to exercise care, maintenance, security and use of the installation activity, or equipment.

FACILITY CLEARANCE

Degree of Clearance	Issuing Office	Date Issued

Contractor personnel employed under this contract shall be required to possess a personnel security clearance. This is a critical requirement.

GOVERNMENT-FURNISHED PROPERTY AND SERVICES

1. Government shall provide to the contractor for use in connection with this contract the following property:

a. Telephones, for official use only--no personal or noncontract performance calls authorized.

b. Heat, light, and other utilities.

c. Security guard working space to include sentry stations, and administrative office space.

d. Standard US Army and Government forms and regulations.

e. Office furniture, to include desks, chairs, filing cabinets, and other related office equipment.

f. An arms container suitable for the security of weapons and equipment when not in use, and magazine storage for ammunition.

g. Base Radio Station.

2. The Government property made available under this contract shall be for official Government use only in the performance of the resulting contract. Government property will be returned on termination of the contract prior to contractor receiving final payment.

3. The Government shall provide normal maintenance and repair of the property furnished to the Contractor under the resulting contract.

Only the material listed above in the quantity shown will be furnished by the Government. All other material required in the performance of this contract shall be furnished by the Contractor.

PLACE OF PERFORMANCE

The Contractor shall perform the services cited herein at ______________ ____which consists of approximately ____acres of land. There are approximately ____ civilian and ____ military employees working at the ____________________________ hereafter referred to as ____________________________.

SCOPE OF THE CONTRACT

The Contractor shall furnish all trained personnel, uniforms, equipment, materials, and supervision with the exception of the Government-furnished facilities, equipment and materials specified herein to satisfactorily maintain the physical security of the ____________________.

In addition to the physical security, the Contractor shall perform such other services as are set forth herein, if any, to insure the safety of the _____________ and all authorized personnel, contractor employees, residents, and authorized visitors.

Services performed under this contract shall be subject to inspection and acceptance by the Contracting Officer or his duly authorized representative. The Provost Marshal/Security Manager is the ______ employee responsible for all security matters at ____ and is the Contracting Officer's Representative (COR). An on-site COR will be designated by the _____ Provost Marshal/Security Manager.

Specific security requirements are given below, and some areas are covered in more detail in the Special Orders and General Orders.

a. The Contractor shall protect all personnel, Government property, material, and equipment from unauthorized use, loss, theft, trespassing, espionage and sabotage, and also protect any and all non-government property located at _________________________________.

b. The Contractor shall control personnel and vehicle entry to and from various entrances at ____________________.

c. The Contractor shall enforce the badge/pass system to identify and control all military and civilian employees and visitors to the installation.

d. The Contractor shall operate a mobile vehicular radio station on a 24-hour, 7 days per week basis for the control of security to quickly and decisively back up any guard who may be confronted with a situation which requires additional personnel.

e. The Contractor shall endeavor to prevent the occurrence of fires, explosions and other catastrophies by close observation of the buildings, machinery, vehicles, electrical equipment, and personnel to identify unsafe or potentially unsafe conditions, procedures or activities.

Upon the citing of any unsafe condition, the shift supervisor shall be notified and admission to the unsafe area shall be by authorized personnel in order to minimize the risk. The shift supervisor shall, in turn, immediately notify the Security Manager or his designated representative, the COR on site.

f. In the event of a fire, the Contractor shall monitor the calls and provide traffic control at the location of the fire.

g. The Contractor shall deter the commission of assaults, batteries, robberies, rapes, and other crimes of violence by deployment of a well trained and organized security force, each member of which will be armed with a .38 caliber revolver and with a personal defense weapon such as a baton.

h. The Contractor shall patrol the entire posted areas of __________ including all parking lots by motor vehicle, or on foot, as required to provide continuous surveillance of the facilities. While patrolling, check all designated gates, doors, and windows, and if gates or doors are found unlocked or windows open, notify the shift supervisor, and close and lock the gates, doors and windows. Also, turn off unnecessary lights and perform other security related activities necessary to meet the overall security requirements of this scope of work.

i. It is mandatory that vehicles be operational and available at all times.

j. The Contractor shall provide security protection in situations such as but not limited to incidents involving drug abuse, alcoholism, psychotic persons, civil disturbances, riots or other disorders. Contractor shall develop and maintain a Guard Recall Bill System capable of recalling cleared guard force members to duty in sufficient numbers to meet emergency situations arising at ________________. The Security Manager, or his designee, will determine what constitutes an emergency situation.

k. Provide escort on and off installation as deemed necessary by the Security Manager or his designee.

l. The Contractor shall enforce all traffic regulations for all vehicles operated on __________________, and direct traffic as required.

m. The Contractor shall make inquiries into incidents and traffic accidents occurring at ______________________within the Contractor's cognizance and verbally report same to the Security Manager. Police traffic accident reports are to be submitted to the Security Manager within 24 hours of the occurrence. The Contractor shall issue speeding citations and report same to Security Manager.

n. The Contractor shall prepare and submit full report of incidents which are considered security breaches, violations of administrative regulations, or the assignment as set forth in the General Orders.

o. The appropriate Contractor guard shift supervisor shall be notified by guards of potentially hazardous conditions and hazardous road conditions.

p. The Contractor shall provide assistance to persons in need of aid involving incidents such as hurricanes, storms, hazardous road conditions, nuisance animals, damaged utilities, and other similar conditions.

q. The Contractor shall receive, secure, and account for all keys issued to the Contractor for use in the performance of this contract. Duplicate or replacement keys must be requested through the Security Manager. Authorized duplicates will be provided at government expense. Keys issued for duty performance will not be removed from the installation.

The Contractor shall maintain records and submit reports in accordance with appropriate regulations, directives and orders (see Special Orders and General Orders) to include, but not limited to, the following:

a. Reports of Inquires into incidents and traffic accidents and speeding citations.

b. Individual guard shift activity summaries and daily journals.

c. Guard Recall Bill.

These completed reports, using military police forms, will be submitted to the provost marshal within 24 hours.

The Contractor shall adhere to the Special Orders which are supplied with this solicitation as attachment. These orders include detailed post and patrol operating procedures covering functions to be performed at each post. These orders may require changes from time to time by the Security Manager, which shall be accomplished on instructions by the Security Manager or his designated COR only. An installation may is also included with this attachment.

The Contractor shall adhere to the Guard Post Manning Requirements which are furnished with this solicitation as attachment. Twenty days prior to entry on duty the Contractor shall supply in writing to the Security Manager an Organization Chart to include the names of the shift supervisors, the shift organization for each post, and the number of guard force employees, along with their respective titles. Thereafter, a monthly roster of personnel assigned shall be submitted on the 30th day of each succeeding month.

The Contractor shall adhere to the General Orders which are supplied with this solicitation as attachment and include many special instructions.

The Contractor will furnish the following: Examples:

a. Main Vehicle Gate: One guard 24 hours every day, plus one guard from 0700 to 1730 hours, Monday through Friday. Guards at this post will check all incoming vehicles. Visitors and delivery trucks will be processed in, given temporary vehicle passes, and directed to their destination. Vehicles owned by ________________ employees will be checked to insure that they are properly registered. The guards will also make spot checks of vehicles departing the installation to insure that no government property is being illegally removed. Proper dispatch of government vehicles will also be checked.

b. West Vehicle Gate: One guard from 1100 to 1300 hours and from 1600 to 1700 hours, Monday through Friday. The guard on this post will be required to perform the same duties as those assigned to the guards on the Main Gate.

c. __________ Gate: One guard from 0700 to 0800 hours and from 1500 to 1700 hours, Monday through Friday. The guards on this post will be required to perform the same duties as those assigned to the guards on the Main Gate.

d. Motor Patrol. One guard 24 hours a day, 7 days a week. It will be the responsibility of the guard on this patrol to check all perimeter roads and fences to insure that no intruder has gained entry to the installation. Further, it will be his responsibility to patrol all parking lots during duty hours and ticket those vehicles in violation of _____________ vehicle registration and parking regulations. The Motor Patrol will also respond to any of the perimeter gates should a guard on one of those posts require assistance. When the necessary equipment has been purchased, it will become the responsibility of the guard on the Motor Patrol to detect personnel violating the posted speed limit on the post by operation of a radar speed gun.

On-site supervision of the Guard Force furnished hereunder shall be provided by the Contractor continuously, around the clock, and shall include inspection of each Post, fixed and mobile, during each shift by the shift supervisor at least twice during each eight-hour (8) period. The Contractor shall provide shift supervisors who will not be assigned to any Guard Post but whose duty shall be to visit and inspect all Posts assigned to the shift. Also, an alternate supervisor for each shift shall be established, who shall serve in the absence of the shift supervisor. The position of guard and that of supervisor cannot be held by the same individual. The shift supervisors shall begin their tours of duty one-half hour prior to the beginning of the shift. An informal guard mount shall be held prior to change of shift. The shift supervisor

shall insure that all guards report for muster on time and that each member of the Guard Force is inspected prior to being posted. Such inspections shall include but are not limited to the following:

a. Complete clean and neat uniform, including shined shoes.

b. Personal appearance acceptable for the police/security profession.

c. Physically capable of standing watch, i.e., not having consumed alcoholic beverages or other types of intoxicants or drugs, and having had sufficient rest.

d. Insure that all guards are properly equipped.

e. Insure that all guards are informed of and understand the Post instructions and all special orders.

In addition to the shift supervisors, the Contractor shall assign a company representative as contact point for liaison between the Contractor and the COR on a 24-hour basis. This company representative is to physically visit the site weekly at random hours and submit, in memorandum form, the results of such visits to the COR.

The Contractor shall maintain a local office where the designated company representative can be contacted during regular working hours by the COR.

QUALIFICATIONS OF PERSONNEL

The Contractor shall insure that all persons employed in the performance of this contract, prior to assignment to duty at ________________ meet or exceed the following minimum criteria:

a. The employee must be at least 21 years of age (age requirement waived for veterans).

b. All employees must have attained a total of any four educational units defined as follows:

(1) Each year of high school completed shall equal one (1) educational unit.

(2) Each year of experience as a "full-time" employee of a military, governmental or civilian security force shall equal one (1) educational unit.

c. All employees assigned by the Contractor to work under this contract shall be physically able to perform all general patrol duties, functions, and activities; shall be free from any communicable disease; shall be well proportioned as to height and weight; shall be in good

general health without physical defects or abnormalities which would interfere with the performance of these duties; shall possess binocular vision correctible to 20/30 (snellen); shall be free of color blindness, and be capable of hearing ordinary conversation at 15 feet with either ear without benefit of a hearing aid. Each employee shall be given a physical examination without cost to the Government or the employee, and medical certification attesting to the final results of this examination shall be furnished to the COR on Standard Form 78 at least five days prior to anticipated date of assignment. This form must receive the approval of the COR prior to assignment of the employee to duty. The furnishing of this certificate, however, shall in no way relieve the Contractor from the obligation imposed upon him as outlined in the first sentence of this subsection. The employee shall be reexamined annually and results furnished to the COR.

d. All employees shall be literate in English to the extent of reading and understanding printed regulations, detailed written orders, training instructions and material, and shall be able to compose reports which convey complete information.

e. All employees must possess the capacity to acquire a good working knowledge of all aspects of contract Security Force position requirements.

f. All employees must qualify as a marksman utilizing the following qualification standard prior to assignment at the activity and annually thereafter:

FIREARMS QUALIFICATION STANDARD

The qualification standard for the course described below is as follows:

Marksman	225 points to 255 points
Sharpshooter	256 points to 280 points
Expert	281 points to 300 points

Stage	Distance	Position	No. Rounds	Stage Time
A	7 yards	Crouch	12 (DA)	25 Secs.
B	25 yards	Standing (No Support)	6 (DA)	12 Secs.
C	25 yards	Sitting Prone Barricade	6 (DA) 6 (DA) 6L (DA) 6R	2 Min. & 45 Secs.
D	25 yards	Kneeling Barricade	6 (DA) 6R (DA)	90 Secs.

((DA) - Double Action) Course - 25 yard course.

The ammunition used may be "Wad Cutter" (for training only) or standard police load ammunition. The Government reserves the right to determine if any contract employee follows established firearms handling practices. Prior to commencement of contract services, Contractor shall certify in writing to the COR that each employee has acquired proficiency in use, care and safe handling of sidearms, and has qualified as outlined above. Thereafter this certification shall be furnished prior to activity.

g. Shift supervisors shall be individuals who have demonstrated supervisory ability by successful experience of at least two years in a position similar to position described hereunder. The Contractor's supervisory personnel in charge of work under this contract shall at all times be available to receive and implement orders or special instructions from the COR which affect the operation or the protection and security of assigned areas.

h. Each guard and supervisor will be required to possess the appropriate valid motor vehicle operator's license to permit the operation of vehicles in the State of ______________________.

The Contractor shall be responsible for maintaining satisfactory standards of employee competency, conduct, appearance, and integrity and shall be responsible for taking such disciplinary action with respect to his employees as may be necessary. Contractor shall immediately report in writing any termination of contract personnel and the cause for such termination.

The Contractor shall insure that Security personnel at all times present a neat appearance, paying particular attention to their personal hygiene, bearing, uniform and equipment. They will keep their hair, mustache and sideburns cleanly trimmed.

REQUIRED CLEARANCES, CERTIFICATIONS, AND ACCEPTANCE (IF APPLICABLE)

The Contractor concurrent with the action of hire, will cause the employee to effect such action and execute such forms as are required by the Defense Industrial Security Clearance Office (DISCO), Columbus, Ohio for requesting personnel security clearance up to and including_________ in accordance with Industrial Security Manual DOD 5220.22-M. (Said document may be obtained from the Superintendent of Documents, US Government Printing Office, Washington, DC 20402.) Prior to assignment of any individual to duty, the Contractor must have satisfactorily completed, administratively processed, and submitted all such required forms to DISCO. The application shall consist of the forms cited in paragraph 26 of the Industrial Security Manual. Five days prior to entry on duty the Contractor shall furnish the Security Officer a consolidated list of all personnel employed under this contract showing the position and degree of personnel security clearance. Thereafter, for each person hired, the Contractor shall furnish the COR a record of the employee's personnel security clearance five days prior to entry on duty.

a. The Security Officer or his designated representative will certify the need for an interim Secret personnel security clearance for a period of 120 days after award of the contract, after which time a request will not be accepted unless detailed justification, for lack of adequate management, is submitted to the Security Manager. The application for interim clearance shall be sent directly to DISCO and the words "Interim ______________" shall be placed in bold letters in the lower right hand corner of the "Job Title and Description of Duties" block of the DD Form 48 or DD Form 49. The Contractor must maintain an adequate nucleus of cleared personnel to cover situations involving vacations, emergencies, etc.

b. For all persons receiving a final or interim personnel security clearance, the Security Officer will issue identification as required for entry to_________________.

All employees of the Contractor employed in the performance of the work under this contract shall be full-time employees of the Contractor at all times and not employees of Government or not members of one of the Armed Services.

UNIFORMS AND EQUIPMENT

The Contractor shall provide for each guard force employee all of the uniforms and personal equipment items outlined below. All contractor guard force personnel shall wear this uniform and all authorized personal equipment while on duty in a clean, serviceable condition. The uniform shall be of a brown, blue, gray, or green color, conforming to acceptable standards and consistent in style and color for each employee. Such uniform and equipment shall include the following:

a. Shirt, or blouse for women, long or short sleeve, a combination of rayon and dacron (not cotton).

b. Trousers, and/or skirts for women, a combination of rayon and/or dacron (not cotton).

c. Jacket, "Ike" or blouse style, a combination of rayon and/or dacron (winter).

d. Cap, military service type, with black visor and rain cover.

e. Raincoat.

f. Belt, trousers, waist, black leather.

g. Socks, black.

h. Shoes, black leather (with plain toes).

i. Ties.

j. Shoulder patches.

k. Boots, rubber.

l. Gloves, black leather.

m. Belt, pistol, black, waist, leather, 1 - 1 1/2".

n. Holster, black leather for revolver with 4" barrel.

o. 38 caliber ammo pouch, belt style.

p. Revolver, 38 caliber, double action, with 4" barrel, blue, steel, US manufacture.

q. Flashlight, three-cell, with batteries.

r. Whistle, chrome, brass, or blue steel.

s. Badge, hat according to rank.

t. Insignia or rank, as appropriate.

u. Name plate, black with white letters.

v. Fiberglass riot helmet with plastic face plate.

w. Police baton.

Female personnel may wear skirts of the same material and color as the male personnel's trousers if such does not substantially interfere with the performance of the assigned duties of the wearer.

Required items of safety apparel will be worn by personnel of both sexes but need not be identical in style but will in each case satisfy the safety standards involved.

Appropriately lettered breast badge and cap ornament indicating the jurisdiction from which police authority is obtained shall be worn and prominently displayed as part of the uniform. Shoulder patches not larger than 4 1/2", lettered to indicate the identity of the Contractor, shall be worn on the left shoulder of the uniform. No other identification of the Contractor is to be worn or displayed on the uniform.

The Contractor shall provide as a minimum the operational equipment outlined below for the use of his employees to execute the provisions of this contract:

a. Six (6) riot shotguns, 12 gauge, with 18" improved cylinder bore, pump operated action, of US manufacture, with number 00 buckshot

ammunition in sufficient quantities for employees training and operational requirements.

b. .38 police special caliber ammunition in sufficient quantity for employee training and operational requirements.

c. Two hand-held portable public address systems with sufficient batteries for employee training and operational requirements.

d. Three hand-held battery operated spotlights with sufficient batteries for employee training and operational requirements.

e. Detex Watch clock (for Post _____) and a total of _____keys.

f. ______vehicles to provide for the Shift Supervisor and Security Patrols as required by the scope of their individual duties. Specifications for these vehicles are given below. (____ estimate of mileage for one year for these _____vehicles is ______miles _______miles per vehicle).

(1) Pick-up trucks, sedans, or station wagons.

(2) Minimum four-cylinder with standard or automatic transmission.

(3) Color white with "Security Patrol" marked on both doors.

(4) Flashing light on roof.

(5) Heater and defroster.

(6) Side view mirror (left and right sides).

(7) Spare tire and tools.

(8) Snow tires/chains (seasonal).

g. Radio equipment, to be compatible with the frequency of the base station, shall include a radio for each patrol vehicle with a remote capability for members of the guard force to utilize when they are required to be away from a patrol vehicle or a telephone.

h. The Contractor should institute a procedure whereby the uniformity of dress of all security personnel within a given duty shift is assured.

GOVERNMENT-FURNISHED PROPERTY

The Contractor shall take all reasonable precautions in accordance with sound industrial security practices to safeguard and protect the Government property and maintain in clean serviceable condition. The Contractor assumes the risk of, and shall be responsible for, any loss of or damage to Government property in his possession except for reasonable

wear and tear and to the extent that such property is consumed in the performance of the contract.

All property furnished by the Government under this contract shall remain the property of the Government, and upon termination of the contract the Contractor shall render an accounting of all such property which has come into his possession under the Contract.

The Government shall not be responsible in any way for damage to the Contractor's supplies, materials, or equipment or to the Contractor employees' personal belongings brought into the building or onto the grounds due to fire, theft, accident, or other disaster.

TRAINING

The required training for the Contractor's employees is broken down into two categories, one to be completed before entering on duty and the second to be completed within thirty (30) days after duty begins. The details relative to this training are given in inclosure ______.

No Contractor personnel shall be on duty on either a fixed or mobile Post for more than twelve (12) consecutive hours in a twenty-four (24) hour period or in excess of sixty (60) hours per week except in an emergency situation and when approved by the Contracting Officer's Representative.

No Contractor employee shall be permitted entry to _______ except to perform assigned guard or supervisory duties.

The Contractor shall not employ any _____ employee to work at ______ in any capacity.

The Contractor shall be responsible for supplying additional guard personnel when required due to special events and/or visits by high ranking military and civilian officials. Each special event shall be for a minimum of two, four or eight hours. The Contractor shall receive advance notification from ____ of these special events, and such notification must be given at least six (6) hours prior to the event.

The Contractor shall be licensed in the State of ______and shall comply with all State and local laws regarding Security Guards.

When special details are formed and any regular posts are designated to be unmanned during the same time frame, special detail manhour rates will be paid only for that number of guards in the special detail who are in excess of the basic manpower requirements for the subject time frame.

FAILURE TO PERFORM

In the event that the Contractor fails to provide a qualified supervisor or guard or allows any post to be unmanned for more than 15 minutes at any time during which shift or special detail said post requires coverage, the following monetary charges shall be made against the Contractor:

a. When a Government employeee of ________is assigned to perform the work required, the Government will deduct from the money due the Contractor the entire cost of the Government employee who performed the work.

b. If no replacement is furnished by _____ and the work is not performed, the Government will deduct from the money due the Contractor an amount equal to the entire cost of the Government employee who would have performed the work.

The documents listed below, including all amendments thereto, are applicable to the contract in administering the security and law enforcement requirements of this contract and one copy will be furnished to the Contractor upon award of the contract: Examples:

a. Reg 190-1, Carpool Parking and Vehicle Registration.

b. Reg 190-3, Preservation of Order Activities.

c. Reg 190-5, Anonymous Calls/Bomb Threat Plan.

d. AR 190-28, Use of Force by Personnel Engaged in Law Enforcement and Security Duties.

e. DOD 5200.1R, Information Security Program Regulation.

f. AR 380-5, Department of the Army Supplement to DOD 5200.1R.

The above documents can be viewed by contacting the Contract Negotiator.

DELIVERIES OR PERFORMANCE

Time of Delivery:

DATA ITEM	DATA REQUIRED
Certification of Refresher Training for each contract employee as set forth in attached roster.	Monthly
Licenses as required by State of ____________________.	On or before five (5) days prior to entry on duty.
Guard Recall Bill System	Within three (3) days prior to entry on duty.
Contractor representative memorandum concerning on-site surveys.	Each week during duration of the contract.
Report on termination of contract employee.	Same day the action is taken.
Reports of investigations into all incidents and traffic accidents	Within twenty-four (24) hours after time of the occurrence of incident or traffic accident.

PLACE OF PERFORMANCE

The place of performance is the Facility Place State.

INSPECTION AND ACCEPTANCE

Services performed under this contract are subject to inspection and acceptance by the Contracting Officer or the COR in strict accordance with preceding specifications.

DISCLOSURE OF INFORMATION

Neither the Contractor nor any of his employees will disclose or cause to be disseminated any information concerning the operation of ____________, which could result in or increase the likelihood or the possibility of a breach of the security of the activity or interrupt the continuity of its operations. Disclosure of information relating to the services hereunder to any person not entitled to receive it, or failure to safeguard any classified information that may come to the Contractor or any person under his control in connection with work under this contract, may subject the Contractor or his employees to criminal liability under Title 18, Section 793 and 798 of the United States Code.

All inquiries, comments or complaints arising from any matter observed, experienced or learned of as a result of or in connection with the performance of this contract and the resolution of which may require the dissemination of official information, will be directed to the Public Affairs Office or to the Duty Officer during nonworking hours. Deviations from or violations of any of the provisions of this subsection may, in addition to all other criminal and civil remedies provided by law, subject the Contractor to immediate termination for default and/or the individuals involved to a withdrawal of the Government's acceptance and approval of employment.

DELEGATION OF AUTHORITY

The cognizant Defense Contract Administration Services Office is hereby designated as the authorized representative of the Contracting Officer for security purposes only.

PROCURING CONTRACTING OFFICER

Contracting Officer
Name
ATTN:
Number, Street
City, State, Zip Code

TECHNICAL COORDINATION LIAISON

The Contractor will not accept any instructions issued by any person other than the Contracting Officer or the Contracting Officer's Representative acting within the limits of their authority. The COR is not authorized to issue any instructions or orders which would require the Contractor to exceed or to perform less than contract requirements. To assure optimum results under this contract, close coordination and liaison between the Contractor's Supervisor and the COR is necessary.

PROHIBITION AGAINST CONTRACT WITH DETECTIVE AGENCIES

Federal law as contained in Section 3108 of Title 5 of the United States Code is quoted as follows: "An individual employed by the Pinkerton Detective Agency or similar organization may not be employed by the Government of the United States or the Government of the District of Columbia." The Comptroller General in his decision B-139965, June 30, 1959 (38 Comp. Gen. 881), held that the above prohibition is applicable to contracts or agreements with detective agencies or agencies which are of an investigative nature, as well as to contracts with individual employees of such agencies, and that the United States Government may not enter into contracts with detective or investigative agencies. In order that award of the contract will not be in violation of the above-cited law, the bidder is requested to complete and sign the certification to this effect.

DETERMINATION OF RESPONSIBILITY

Award of the contract to a potential supplier is not based on the lowest evaluation price alone. Due consideration shall be given to those standards for responsible prospective Contractors, as set forth in ASPR 1-900, including (a) adequate financial resources, (b) ability to comply with required performance schedules while taking into consideration existing business commitments, (c) satisfactory records of previous performance, (d) satisfactory record of integrity, and (e) otherwise eligible to receive an award under applicable law and regulations. If the offer outlined herein is favorably considered, a survey team may contact your facility for the purpose of determining your financial and technical ability to perform.

Bidder shall supply a brief resume of previous and current performance, over a five-year period, listing the agencies and companies with whom they have contracted, their addresses, the contract numbers, and the manpower level required for each contract.

To enable the Government to determine responsibility, the bidder may be asked subsequent to bid opening to furnish a statement as to the present financial condition of the company, as well as the financial resources available to cover start-up expenses should a contract be awarded.

TRAINING

1. All employees shall be required to satisfactorily complete the following minimum training prior to post assignment, and written certification shall be supplied to the COR three (3) days prior to the date the Contractor commences duty at ____________. Thereafter, certifications for any new contract employee shall be supplied prior to the time that employee reports for duty.

a. Mission and function of security guard operations

Purpose and duties of security guards.

b. Post Orders

Thorough understanding of General & Special Orders and other provisions of the contract.

c. ID Badge System

Employee badge, visitor badge, and automobile pass.

d. Safeguarding Classified Material

The protection and transmittal of classified material.

e. Security Guard Authority

Power to arrest, detain and search.

f. Basic Firefighting

Use of fire alarm system, fire extinguishers and fire barriers, and sprinkler systems.

g. Elementary first aid.

h. Pistol/Revolver Qualification

Safe handling, condition of use and record firing with small arms.

i. Report Writing

(1) Writing clear and concise reports--who, what, when, where, why, and how.

(2) Military time (24-hour clock) and day-month-year notations used in all reports.

j. Guard Orientation

General orientation on conduct and attitudes on and toward the job.

2. Additional training shall be satisfactorily completed in the following subject areas within thirty (30) days of entering on duty by all employees. This training is only a minimum and shall be certified in writing by the Contractor.

a. Radio Procedure

Standard police radio 10-series code system.

b. Traffic Control

Movement and control of vehicular traffic by guard using hand and arm signals.

c. Methods of Pilferage, Sabotage, Espionage, and Other Criminal Acts.

Methods of prevention, detection, apprehension, use of deadly force, and self-defense.

d. Bomb Threats

Search methods, plans, and evacuation of buildings.

e. Disaster Preparedness

Maintenance of law and order and suppression of unlawful acts in times of disaster.

f. Civil Disturbance and Riot Control

Protection of property, closely controlled access, and use of barriers.

g. Standards of Conduct

Performance standards which promote high duty performance.

h. Familiarization with Riot Control Agents/Weapons

Familiarization with procedures as provided in Civil Disturbance Plan.

i. Explosives Safety and Radiation Hazards

(1) Familiarity with all restrictive signs and symbols, their meaning and absolute compliance with them.

(2) Dangers inherent in fires associated with explosives and radioactive equipment, and safety through time and distance.

j. Contingency Plans

Hostage negotiation techniques, tactical response to terrorist activity.

k. Discipline

l. Public Relations

3. Each security guard and supervisor shall receive 3 hours of refresher training each month throughout the duration of the contract, and the type and completion of training certified in writing by Contractor to the COR.

4. Each employee shall be qualified in the use and safe handling of firearms. The minimum proficiency in weapons use will be as given in Firearms Qualification Standard. This proficiency shall be established by supervised and recorded firing and shall be maintained during the contract performance period. Qualifications shall be at least once during each calendar year and certification submitted.

5. Time and material costs for training purposes shall be borne by the Contractor and all training certified by the Contractor.

SAMPLE ORDER

US Army Materiel Development
& Readiness Command

Special Order # (1)
Date:

Name
City, State

SECURITY BRANCH ORDER

Subject: Installation Perimeter Detex Key Station Clock Patrol Post #____________.

1. The person on patrol who is carrying the clock on Post #________, will, during the course of his route be especially observant for trespassers, building security, fire and any safety hazards that should be reported for correction.

2. The following specific items will identify the route of the patrol and security checks to be made en route to and departure from each location:

ITEM	KEY	LOCATION	SECURITY REQUIREMENT
1	20	North of Bldg. West side of Parking Lot area.	Depart from Main Guard Office Proceed along North Avenue in a westerly direction. Check the North Parking Lot and exterior doors of Bldg. #_____ north side. Proceed to Key #_______ Check this area to include north, west, east and south side of Bldg. #______________.
2	21	Perimeter fence center of South Parking Lot along perimeter roadway boarding Army Reserve Center.	Proceed to Key #_________via South Avenue along Bldg. # ______________South and enter perimeter road south of Bldg. #____________, Main Gate Guard Building. Continue along the perimeter fence and check the South Parking Lot, Bldg #_______ and proceed to Key #___________.
3	2	West of exit Service Gate roadway	Check both Service Gates Entry/Exit, Bldg. #_________Ser-Gate Guard Bldg. Visually check the Motor Pool Parking Lot while proceeding to Key #__________.

US Army Materiel Development & Readiness Command

Special Order # (1) Continued
Date:

ITEM	KEY	LOCATION	SECURITY REQUIREMENT
4	23	West perimeter fence North corner at connecting gate areas	En route to this Key check the perimeter fence for holes, damage or suspected forced entry.
5	24	Exit roadway-East perimeter side of________ Drive beyond ______________.	Returning from Key #_____enter ________Drive, proceed through South Parking Lot exiting at South Avenue. Continue on to ___________Drive north to exit/entry roadway East perimeter fence to Key #_______________.
6	25	Adjacent to Service Gate Guard Bldg. Z _____Road vehicular gateway.	Check area en route to include East perimeter fence. Check the X________Hill road Vehicular Gates and the Guard Bldg. Visually check the Tank Far rear of Bldg. #________. Check the Pedestrian and Vehicular/Electrically controlled gate leading into the ______________ Facility.
7	26	East side of Bldg. #______ - South of Loading/Unloading Platform.	Check the area East, South, West, and North of this Bldg. Check the Pedestrian Gate connecting with Bldg. #_________ _________________Facility.
8	27	West of Vehicular entry gate to Bldg. #__________ Explosive Load & Test Bldg. Area.	Proceed to Key #________via Flor Drive South and turn West on Kuester Road going West. Check the area en route for trespassers. Check the Vehicular Gates leading into Bldg #A, #B, #C, Check Bldg. #D and surrounding area. Return via ____________Road and_________ Drive to the Main Guard Office.

US Army Materiel Development
& Readiness Command

Special Order # (1) Continued
Date:

3. Installation perimeter Detex Key Station Clock Keys are mounted on numbered, traffic orange posts, at the locations indicated above.

4. On Monday through Friday a minimum of two (2) perimeter clock patrols will be made by Watch #3 and three (3) perimeter clock patrols will be made by Watch #1. On Saturdays, Sundays and Holidays three, each, clock patrols per Watch will be made on a continuing twenty-four (24) basis.

5. The Supervisor on duty at 0800 hours daily Monday through Friday or his designated representative, will change the clock disc. The Captain will assume the responsibility of checking each clock disc to ascertain that the required patrols and designated key station checks were made. On Saturdays, Sundays and Holidays, Supervisor on duty, or the OIC, Watch #2, will change the clock disc at 0800 hours. Clock discs reflecting these days will be placed into the In-Box of the Captain for his review on his next scheduled work day.

6. Clock Discs for all Detex Clock patrols internal, external as well as the Nike Site (Post #11) will be retained in the Office of the Captain.

FOR THE COMMANDER:

JOHN E. SAFE
Chief, Security Branch

SAMPLE ORDER

US Army Materiel Development
& Readiness Command

Special Order # (2)
Date:

Name
City, State
SECURITY BRANCH

ORDER

Subject: Guard Procedures for Operation of Post #_______(Vehicle Gate), Bldg.__________.

The guard assigned to Post #________ will operate the post in accordance with the following instructions:

1. The entrance gate will remain closed at all times.

2. The exit gate will be opened from 1100-1300 and 1600-1700, Monday through Friday.

3. ___________personnel/vehicles will be allowed to exit only from this gate during hours of operation. Each vehicle exiting this post will be checked for ________ bumper decals and allowed to exit.

4. Visitors, contractors, and commercial carriers will not be allowed to exit via this gate. If a visitor, contractor, or commercial carrier attempts to exit from this gate, they will be directed to the Main Gate, Post #__________.

5. Random vehicle searches may be conducted in accordance with the provisions of General Order #_________covering vehicle searches at ___________.

6. Guard will visually check vehicles for government property not coming from the Restricted Area. In order to allow government property from the installation, the property must be accompanied by a DA Form 1818, Individual Property Pass. When the DA Form 1818 is presented, the guard will check for an authorized signature contained in the signature card box maintained at the post. An authorized signature on DD Form 577, Signature Card, must appear on DA Form 1818 to allow the property to pass. If an authorized signature is on file, the guard will compare the property to the property described on the pass and allow the person to remove the property from the installation. If the government property is not covered by a pass or the pass does not contain an authorized signature, the guard will contact the COR for instructions. The guard will detain the person and property until instructions are received from the COR concerning disposition. The DA Form 1818 must be taken up by the guard on duty and a log entry made. The pass will be turned over to the COR at the end of the guard tour.

7. In the event an alarm is received by the guard from the COR, the guard will immediately secure the gate and wait for further instructions from the COR.

US Army Materiel Development
& Readiness Command

Special Order # (2) Continued
Date:

8. Any questions or situations arising while this post is in operation which are not covered by these instructions will be directed to the COR for resolution.

FOR THE COMMANDER:

JOHN E. SAFE
Chief, Security Branch

SAMPLE ORDER

US Army Materiel Development
& Readiness Command

Permanent Order # (1)
Date:

Name
City, State

SECURITY BRANCH ORDER

SUBJECT: Duty Hours of Guard Force

Duty hours for Guard Force personnel are as follows:

First Watch	From	2245 to 0645 hours
Second Watch	From	0645 to 1445 hours
Third Watch	From	1445 to 2245 hours

FOR THE COMMANDER:

JOHN E. SAFE
Chief, Security Branch

SAMPLE ORDER

US Army Materiel Development
& Readiness Command

Permanent Order # (2)
Date:

Name
City, State

SECURITY BRANCH

ORDER

SUBJECT: Motor Pool Vehicle Security Check

1. A check of all Government vehicles parked in the area south of Bldg. _______ will be made shortly after the close of each workday. Government vehicles will be inspected to assure that all doors are locked, windows are closed, key is not left in the ignition, and that no classified papers or hardware have been left therein.

2. Any Government vehicle found open by the guard will be manually secured. A written report in duplicate, encompassing the following information will be made and reported to the Supervisor and COR prior to close of business, Watch #3.

3. In addition to written report required in paragraph 2, Supervisor will make a brief Guard Log Book entry when a Government vehicle is discovered unsecured. Log Book entry will be substantially as follows: "Government vehicle - serial number - and license number found unsecured."

4. In the event of inclement weather, such inspection will be made promptly at 1645 hours.

FOR THE COMMANDER:

JOHN E. SAFE
Chief, Security Branch

SAMPLE ORDER

US Army Materiel Development
& Readiness Command

Permanent Order # (3)
Date:

Name
City, State

SECURITY BRANCH

ORDER

SUBJECT: Post Department

1. Literature: Newspapers, magazines, or other unofficial printed material will not be kept or used on any post by members of the Guard Force.

2. Televisions: Television receivers are not authorized for use on any post or any watch.

3. Appearance: Guards will present a neat appearance at all times with uniform kept cleaned and pressed and complete. Jackets may be taken off during hot weather but, when worn, will be kept buttoned.

4. Loiterers: No guests or visitors will be permitted to enter that portion of Post #_____ which constitutes the Guard Office, or to loiter at any other fixed post maintained by guards. Polite but firm refusal must be given all personnel that endeavor to engage the guard in unofficial conversation while on post.

FOR THE COMMANDER:

JOHN E. SAFE
Chief, Security Branch

SAMPLE ORDER

US Army Materiel Development
& Readiness Command

Special Order # (3)
Date:

Name
City, State

SECURITY BRANCH ORDER

SUBJECT: Guard Procedures for Operation of Post #__________Gate.

The guard assigned to Post #__________will operate the post in accordance with the following instructions.

1. This post will be in operation from 0700-0800 and 1600-1700, Monday through Friday. This post will allow entrance only of personnel/vehicles from 0700-0800 and exit only for _______vehicles from 1600-1700.

(a) From 0700-0800, guard will allow to enter the installation only those personnel/vehicles assigned to ________. The guard will check vehicles for proper bumper decals (registration and insurance) and NSWC vehicles for proper bumper decals. Guard will check all occupants for either an _____employee badge. Personnel without proper badges or vehicles without proper decals will not be allowed to enter and will be directed to the Main Gate, Post #_________Road, not through the installation.

(b) From 1600-1700, guard will allow_____vehicles with proper decals to exit from the installation. The guard will not check security badges for vehicles exiting the installation.

2. Visitors, contractors, and commercial carriers are not allowed to use this gate at any time. All visitors, contractors, and commercial carriers attempting to enter or exit via this gate will be directed to the Main Gate, Post #_________.

3. Random vehicle searches may be conducted in accordance with the provisions of General Order #______ covering vehicle searches at __________.

4. Guard will visually check vehicles for government property not coming from the Restricted Area. In order to allow government property to pass from the installation, the property must be accompanied by DA Form 1818, Individual Property Pass. When the DA Form 1818 is presented, the guard will check for an authorized signature contained in the signature card box maintained at the post. An authorized signature on DD Form 577, Signature Card, must appear on DA Form 1818 to allow the property to pass. If an authorized signature is on file, the guard will compare the property to the property described on the pass and allow the person to remove the property from the installation. If the government property

US Army Materiel Development
& Readiness Command

Special Order # (3) Continued
Date:

is not covered by a pass or the pass does not contain an authorized signature, the guard will contact the COR for instructions. The guard will detain the person and the property until instructions are received from the COR concerning disposition. The DA Form 1818 must be taken up by the guard on duty and a log entry made. The pass will be turned over to the COR at the end of the guard tour.

5. In the event an alarm is received by the guard from the COR, the guard will immediately secure the gate and wait for further instructions from the COR.

6. Any questions or situations arising while this post is in operation which are not covered by these instructions will be directed to the COR for resolution.

FOR THE COMMANDER:

JOHN E. SAFE
Chief, Security Branch

SAMPLE ORDER

US Army Materiel Development
& Readiness Command

Permanent Order # (4)
Date:

Name
City, State

SECURITY BRANCH ORDER

SUBJECT: Duties Post __________Main Gate

1. The Main Gate to the _______________, Post #_________will be manned by one (1) guard on a 24-hour a day basis. In addition, a second guard will be on duty at the Main Gate from 0700 to 1700 hours, Monday thru Friday.

2. Private Vehicles:

Personnel assigned to Post __________ are responsible for checking all incoming and outgoing vehicles. Private vehicles belonging to employees must bear an ________Vehicle Registration Decal in addition to a current Insurance Decal. Incoming vehicles that do not have these decals will be stopped by the guards on duty. If the vehicle is owned by an ___________ employee, he will be instructed to proceed directly to the Main Guard Office and properly register the vehicle. Should there be a valid reason why the vehicle cannot, at that moment, be registered, the owner will be issued a Temporary Parking Pass and advised to register the vehicle as soon as possible. Non-employees arriving at the installation on official business, will be issued a Temporary Parking Pass and directed to those areas set aside for Visitor Parking. All Temporary Parking Passes, whether issued to ________employees or non-employees, will be surrendered to the guard on duty at the Main Gate when the bearer departs the installation.

3. Commercial Vehicles:

a. All commercial vehicles will enter the installation via the Main Gate. The truck and driver will be registered by the guard at time of entry by use of a vehicle registration form and the vehicle will be searched for contraband articles, incendiary devices, hazardous items and unauthorized personnel. The driver will then be directed to the Shipping and Receiving Section, Bldg 102, by the most direct route available. The driver will also be informed that he is to return to the Main Gate immediately after completing his transaction at Bldg. 102. At time of departure, the vehicle will again be searched to insure that outgoing cargo is in accordance with shipping documentation. Vehicles will not be allowed to proceed until any existing discrepancies have been resolved, and ___________Form ________ has been surrendered to the guard on duty.

b. The register mentioned in paragraph 3 above will be a serially numbered controlled form executed in duplicate for each truck entering the installation, the original form signed by the supervisor on duty at all points where pickups and/or deliveries are made. In addition, the supervisor will note the type of cargo loaded or unloaded. This form will

US Army Materiel Development
& Readiness Command

Permanent Order # (4) Continued
Date:

be returned to the guard when the driver returns to the gate. Duplicates will be maintained by the guards on duty and will act as the truck register for that tour of duty. The originals, when returned will be matched to corresponding duplicates.

c. Sealed vehicles will be examined to insure that the seal has not been tampered with and seal numbers will be recorded on the Truck Register. Vehicles with broken seals or whose seal number does not correspond with shipping documentation, will be examined in accordance with paragraph 3a above.

4. Vehicle Searches:

a. In addition to conducting searches of commercial vehicles, Security Guards posted at the Main Gate will also conduct periodic spot searches of private vehicles both entering and exiting the installation. Guards will be especially observant in checking for items of Government property being removed from the installation, as well as unauthorized items being brought onto the installation (refer to 3a above for examples). Government property being removed from the installation must be accompanied by a DA Form 1818, Individual Property Pass. The signature on the DA 1818 must correspond to one in the guard's file of "Authorized Signature Card," DD Form 577

b. Should the guard on duty be confronted with a vehicle carrying either Government property or unauthorized property into or out of the installation, in other than the prescribed manner, he will direct the operator of that vehicle to pull it out of line of traffic and then contact the COR for further instructions. A post blotter will be maintained at Post 7 of all transactions at this post.

c. The guard on duty at the exit point will check the Government vehicle trip ticket to insure that the vehicle has been properly dispatched.

FOR THE COMMANDER:

JOHN E. SAFE
Chief, Security Branch

US Army Materiel Development
& Readiness Command

Permanent Order # (5)
Date:

Name
City, State

SECURITY BRANCH ORDER

SUBJECT: Use of Force - Restrained and Deadly - By Personnel Engaged in the Performance of Security Duties

1. Guard force personnel will at times attempt to discharge their duties without resorting to the use of force. Should it become impossible to do so, then only the minimum amount of force reasonably necessary will be employed. Deadly force, which is that physical force that may cause death, will be used only when all other means have failed, and then only under the following circumstances:

a. Self-Defense: When guard force personnel reasonably believe themselves to be in immediate danger of death or serious injury.

b. Prevent the theft of, damage to, or espionage aimed at property and/or information designated by the Commander as being either vital to, or of substantial importance to, the National Security. At the ________________ areas containing such property and information are as follows:

(1) Property and information vital to the National Security:

None

(2) Property and information of substantial importance to the National Security:

Bldg.

c. Prevent the theft of or sabotage to property which is inherently dangerous to others.

Bldg.

d. Serious Offenses Against a Person(s): When guard force personnel reasonably believe that a serious offense is about to be committed against a person or persons, that involves death or serious bodily harm (examples are armed robbery, aggravated assault, rape, arson, and bombing).

e. Apprehension - When guard force personnel reasonably believe that it is necessary to apprehend an individual responsible for one or more of the offenses listed in b, c, and d above.

US Army Materiel Development
& Readiness Command

Permanent Order # (5) Continued
Date:

f. Escape: When guard force personnel reasonably believe that it is necessary to prevent the escape of an individual who is responsible for one or more of the offenses listed in b, c, and d above.

g. Lawful Order: When directed by the lawful order of a superior authority who shall be governed by the criteria detailed above and AR 190-28.

2. Legal guidance that may be required concerning the apprehension of unauthorized intruders will be furnished by telephoning one of the following, in the order listed:

Mr. A. A. Law	-	Chief, Office of Legal Counsel,	Office #:123-4567 Home Tel:765-4321
Mr. Bob Judge	-	Assistant, Legal Counsel	Office #:123-4567 Home Tel:765-4321

FOR THE COMMANDER:

JOHN E. SAFE
Chief, Security Office

SAMPLE ORDER

US Army Materiel Development
& Readiness Command

Permanent Order # (6)
Date:

Name
City, State

SECURITY BRANCH ORDER

SUBJECT: Bomb Threat Procedures - Post #____________.

1. Security Guards receiving a telephone bomb threat will:

(a) Remain calm - bomb threats are usually received in sufficient time to permit evacuation of the area.

(b) Listen carefully for any unusual characteristics in the caller's voice as well as background sounds that might aid in locating the place from which the call was made.

(c) Be alert of the use of certain words or phrases.

(d) Record the date and precise time the threat was received.

(e) Listen for any accent in the voice of the caller.

2. The Security Guard will make every attempt to obtain the following from the caller:

(a) Where has the explosive device been placed?

(b) At what time is the device set to detonate?

(c) What does the device look like?

(d) What type of explosive material was used in the device?

(e) How will the device be detonated?

(f) Why was the device placed at ___________?

3. After securing all available information from the caller, the Security Guard will immediately call the COR and thoroughly brief him on the available facts.

FOR THE COMMANDER:

JOHN E. SAFE
Chief, Security Branch

US Army Materiel Development
& Readiness Command

Permanent Order # (7)
Date:

Name
City, State

SECURITY BRANCH ORDER

SUBJECT: Non-Duty Hours Admission Procedures - Post #

During out of hours periods (1730 to 0700, Monday through Friday) as well as on weekends and holidays, the Security Guard on duty at the Main Gate, Post _______, will be responsible for registering all incoming and outgoing personnel. All personnel arriving at the Main Gate during these periods will be required to sign in on the Visitor's Registration Log which will be maintained at Post #____________. They will print their name, give destination, reason for coming in, and time of arrival. After this, the employee will be allowed to proceed. Upon departing the installation, the employee will stop at Post #___________and enter his time of departure and signature on the log.

FOR THE COMMANDER:

JOHN E. SAFE
Chief, Security Branch

SAMPLE ORDER

US Army Materiel Development
& Readiness Command

Permanent Order # (8)
Date:

Name
City, State

SECURITY BRANCH

ORDER

SUBJECT: Parking Violation Inspection

1. Inspection will be made at least two times per shift on Watch #2 and Watch #3 of the following parking areas to assure compliance with parking regulations set forth in __________Regulation __________.

(a) North parking lot (north side Bldg ___________ and South parking lot (south side Bldg__________and that area north of Bldg _______and south of Bldg ___________as indicated on site map.

(b) Small car parking which comprises the last three rows at the east end of the South parking lot.

(c) Reserved parking in front of Building 205 (Government vehicles only) and other reserved parking as indicated by yellow "R."

2. It is the responsibility of the Supervisor of each watch to enforce parking regulations for all areas of the installation and to issue violation notices as required. The Supervisor will forward the copies of violation notices to the COR at the end of each watch.

FOR THE COMMANDER:

JOHN E. SAFE
Chief, Security Branch

SAMPLE CHART

US Army Materiel Development
& Readiness Command
Name, City, State

Security Guard Manning Chart

Adelphi

Post Location	Personnel	Hrs/Day	Days/Week	Weeks/Year
Supervisor	1	24	7	52
#7 - Main Gate	1	24	7	52
#7 - Main Gate	1	10	5	52
#8 - Vehicle Gate	1	3	5	52
#9 - Motor Patrol	1	24	7	52
#14- ______ Gate	1	2	5	52

JOHN E. SAFE
Chief, Security Branch

Appendix H

Game Warden's Role



The installation game warden, in his execution of fish and wildlife law enforcement duties, should be used to supplement the physical security program in remote areas of the installation. Game warden personnel have the ground mobile capability to enhance the security posture during daylight and darkness in areas normally inaccessible or off limits to "white-hat" patrols. This appendix outlines the areas of assistance in which security can be supplemented by game war-

H-1 Signs

a. Game warden personnel should detect and report sign damage and recommend sign posting at:

(1) Installation boundaries

(2) Off limits and restricted areas

(3) Routine access areas by public personnel

(4) Hunting and recreational areas.

b. Coordinating sign maintenance is a continuous process in support of the installation security posture.

H-2 Natural Disasters

a. Game wardens can be used in assessing damage from:

- ☐ Fire
- ☐ Flood
- ☐ Storm
- ☐ Wind.

b. The game warden can recommend, due to damage assessed, where to position security forces in support of area facility, and perimeter security to enhance the overall security posture.

H-3 Isolated Areas

Fish and wildlife personnel can also assist in detecting planned criminal activity such as:

a. Larceny of government property and equipment.

b. Operation of covert illicit activities (liquor stills, drug drops, staging areas for terrorist activities, etc.).

c. Provide assistance in detecting trespassing of personnel or individuals loitering in out-of-the-way places

d. Detect unsecured buildings and report and supervise the repair of physical barriers.

e. Assist in security of downed aircraft.

f. Periodic spot checks of POVs to prevent transportation of ammunition from ranges off post.

H-4 Detect Pilferage

In the following:

- Semi-isolated and isolated work areas
- Range areas
- Warehouses
- Open storage construction yards
- Rail yards.

H-5 Equipment

Game wardens assisting in the security program should have the following equipment:

a. Ground motor vehicle with off road capability.

b. Vehicle communications with a recharge/disconnect capability for extended remote operations.

c. Proper seasonal protective clothing.

d. Participate as an observer on rotary-wing aircraft to conduct security assessments and surveillance.

e. Armed and badged.

H-6 Routine Observation

- Post boundary
- Range areas and buildings
- Pipelines
- Pump station
- Bulk storage areas
- Communication facilities/lines
- Lake/river docks
- Government boats
- Recreational areas
- Physical security plan
- All security activities
- Related duties in FM 19-10.

H-7 Security Awareness

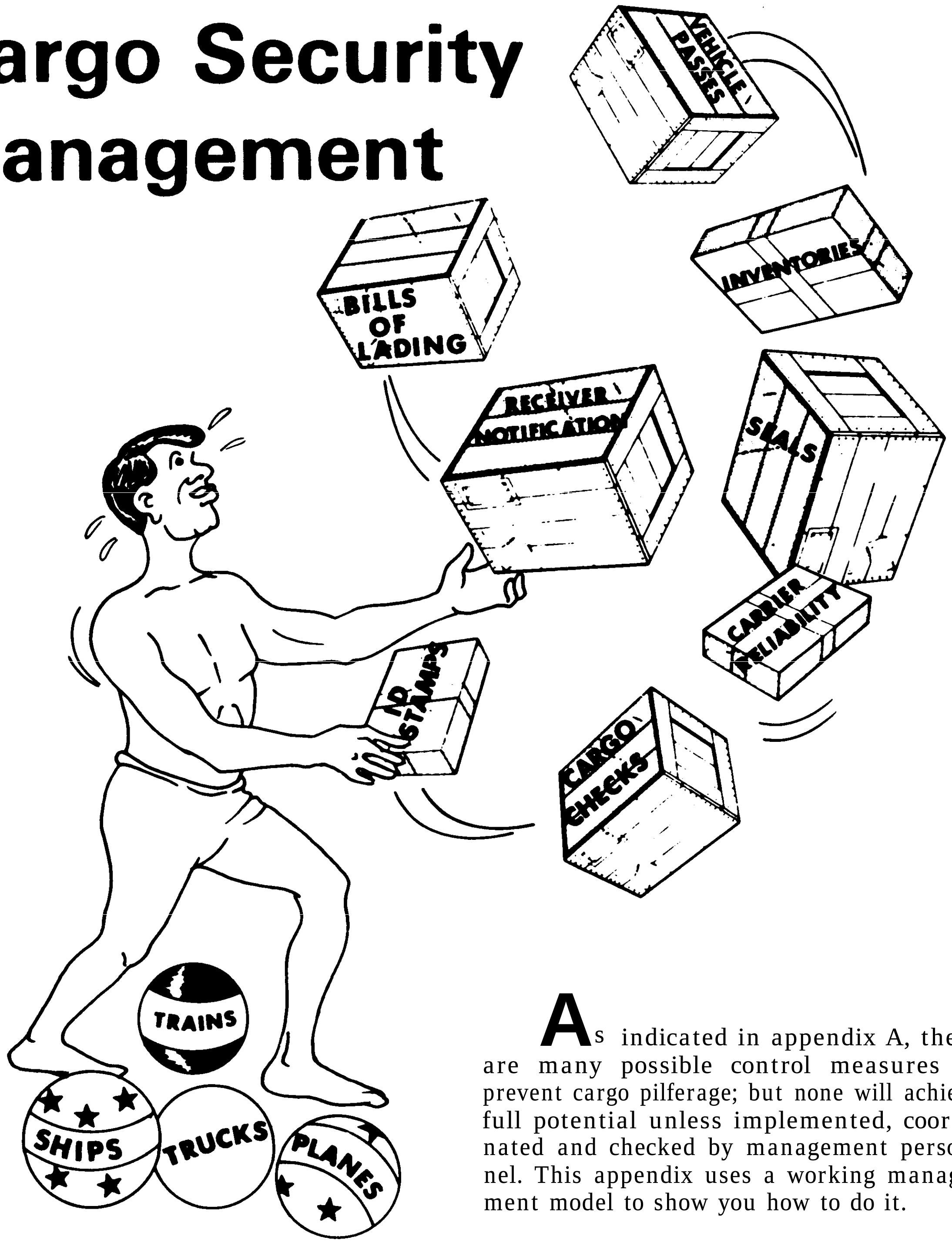
Be familiar with the requirements in AR 190-13, FM 19-30, plus command policies and directives.

H-8 Additional Information

The special package produced for the military police platoon leader's course, Fort McClellan, Alabama is an in-depth discussion of wildlife law enforcement.

Appendix I

Cargo Security Management



As indicated in appendix A, there are many possible control measures to prevent cargo pilferage; but none will achieve full potential unless implemented, coordinated and checked by management personnel. This appendix uses a working management model to show you how to do it.

I-1 Cardpac

A good illustration of cargo security integrated management is the Military Traffic Management and Terminal Service (MTMTS) card packet system. (MTMTS is a Department of Defense agency that centralizes and coordinates the procurement and operation of transportation services for the movement of military freight and personnel.) The computerized card packet system, Cardpac, was designed to operate at six high volume marine terminals, through which about 85 percent of the MTMTS surface export cargo flows.

When a DOD shipper alerts the computer at an MTMTS area command that a shipment destined for overseas is in the transportation pipeline, this information is relayed by the area command to the computer at the water terminal scheduled to receive the shipment for export. The terminal's computer automatically generates a set of punched cards containing all the data necessary for terminal personnel to process the incoming shipment. These cards are the basis for management printouts for controlling the cargo as it moves through the terminal and are the means by which to update the area command master file.

When the shipment is received, one of the prepared cards is used as a receipt document. The checker at the gate records the date of receipt and the location within the terminal where the cargo is stored.

I-2 Consignee Management

a. Consignee management should instruct its **receiving department to notify purchasing when incoming items arrive.** This helps prevent fraudulent purchase orders originated by someone outside of purchasing from getting into the flow and forces receiving to make a careful count.

b. To help assure timely detection of thefts occurring before goods get into the consignee's record system, **request purchasing personnel to contact the supplier directly when an order is not filled within a reasonable time.**

c. To prevent forged purchase orders and subsequent thefts, **prohibit purchasing department from receiving ordered merchandise** from having access to such merchandise. Likewise, assure that receiving personnel do not perform purchasing duties.

d. Only specified individuals should be authorized to check in merchandise received. Unless responsibility is fixed, shortages can be blamed on others.

e. Consignee **employees who check incoming goods should reconcile such goods with a purchase order and remove goods to the storage area immediately** thereafter. Absence of a purchase order could mean the merchandise was ordered fraudulently with the intention of removing it before it got into the record flow. Prompt transfer of goods to storage not only gets them into the record flow, but also removes them from a traditionally high-theft area.

f. Consignees should not delay taking delivery of goods. Anticipate difficulties regarding import license, exchange control, or other regulations. Those who have taken advantage of free time in customs and of free storage time at earner terminals often find that the practice is penny-wise but pound-foolish. For example, an importer of canned goods took prompt delivery and suffered only limited pilferage in contrast to the heavy losses of his procrastinating competitors.

I-3 Receiving

a. Receiving personnel should use **prenumbered forms on which to record delivered merchandise, and copies**

153-846 0 - 94 - 15

should be sent to purchasing and accounts payable. This will help deter destruction of receiving records and theft of merchandise. Failure to furnish purchasing with a record will spur an investigation, and failure to advise accounts payable will result in a complaint by the supplier.

b. All discrepancies must be immediately reported to the terminal manager and/or security director for investigation.

c. Freight received without accompanying documentation should be stored in a secure place. Record the number of shipping documents given to strippers or loaders. When the documents are returned, count them again and compare totals.

d. When returned by the local driver, **delivery receipts** should be **compared with terminal control copies** and all bills accounted for.

e. Analyze claims to determine type of cargo most subject to theft and where it's being lost.

f. Each receiving station should assign a trusted employee to **review advance manifests** or, if none, the documents arriving with the cargo to identify and segregate for special attention theft-prone cargo. Such "paper alerts" should also be supplemented by actual examination of the cargo. For example, a manifest described one shipment as "electrical equipment," but the carton identified the goods as calculators. Relying on the manifest, a cargo handler treated the shipment as general cargo; one of the calculators was later stolen.

g. Cargo entering a terminal from shippers or other stations should be thoroughly inspected, accurately counted, properly classified, and immediately stored. Paperwork should reflect all decisions and actions taken.

h. Require **positive identification from pickup drivers to** insure they are the legal representatives of the carrier. Record license numbers, especially on rental vehicles.

I-4 Shipping

a. Prepare **legible bills of lading** and other shipping documents, which are manufactured from a paper stock that will hold up under multiple handlings. Try to use classification descriptions instead of trade names, and avoid listing values.

b. Periodically, **rotate drivers among runs. Otherwise, there** is too great a chance that they might develop contacts for collusion. Beware of drivers who request certain routes despite the lower wages associated with those routes.

c. Change truck stops frequently.

d. Develop **incentive plans to control losses–** payments to employees being based on reductions in insurance premiums and/or actual losses.

e. On multipiece shipments, shippers should **label each package.** As the driver instruction manual of one carrier reads, "The driver must check all shipments to determine that each piece is legibly, durably, and properly marked. The name and address of the shipper must be shown on each piece of freight in any shipment. The marking on each article should be checked to determine if the consignee's name and address is the same as shown on the airbill. Drivers must be certain that the marking will not tear off when the shipment is in transit."

f. Exposure to loss often increases with higher **turnover of personnel** on shipping and receiving docks.

g. Segregate shipping from receiving areas, inbound and outbound cargo.

h. Any employee withdrawing goods from storage should be different from the one actually releasing the merchandise (appendix A).

1-5 Security Education

Security education should consider the risk analysis aspects outlined in chapter 1 and be constructed as defined in chapter 2, Security Education.

a. As practicable, **insist on piece counts when cargo is moved to** and from vehicles and in and out of storage areas, vessels, railcars, aircraft, etc. And insist on clear identification of those who conduct such counts-driver, checker, receiving personnel, terminal cargo handler, or whoever. The two parties involved in a cargo transfer should not take one another's word regarding the count. If they do, accountability becomes blurred.

As a carrier executive advised, employees who check cargo must be told, "You are individually responsible. You must know. You must count." Among his instructions to drivers were these: (1) "If the bill calls for 'CS. No. 1234,' don't accept a case marked '4567' for it." (2) "A driver should never accept a shipment described as 'one bundle tires.' The airbill should indicate how many articles are in the bundle. For example, 'one bundle (4) tires.'" (3) If a shortage exists in a shipment, determine the exact piece short. "If it is shoes, the exception should be '1 cs. shoes short.' A general statement such as '1 cs. short' is not sufficient...."

b. Negotiate with carriers for what one large shipper calls **"signature security service"** for certain kinds of shipments. This means a signature and tally are required from each person handling the shipment at each stage of its transit, from point of origin to destination.

c. Prelodged delivery or pickup order should be safeguarded from theft or unauthorized observation. **Verify identity of carrier and carrier employee** before releasing a prelodged pickup order.

An operator of large terminals notes the potential advantages of prelodging: "We encourage truckers to bring their documentation to the terminal the day before they deliver cargo. We prepare our receiving documents from the trucker's papers and when trucks arrive, give priority in handling to the loads for which we were furnished advanced documentation. Cargo handling is expedited, checking is more precise, and the documents themselves are more accurate. Our cargo accounting has improved significantly...."

This confirms the observation in a carrier task force report: "Reforms in paperwork to eliminate bottlenecks and to raise accuracy also may make it less easy to smudge the responsibility for cargo and cargo records."

d. Restrict access to cargo documentation to a need-to-know basis. Systems assuring strict accountability for documentation are as important as those designed for the cargo itself.

For example, after several thefts in a terminal involving stolen documentation as well as its cargo, an internal release order was devised. The cargo handler who is to retrieve a shipment in the terminal is given the release order, which describes the cargo and its location. Source documents remain in the order. The clerk retains a copy of the release on which he records time of preparation and name of the cargo handler. The cargo handler takes the shipment to his control supervisor, who verifies the identity of the cargo handler and description and quantity of cargo to be delivered. The supervisor requests the signature of the trucker after recording date and time of release. Finally, the release order is returned to the clerk who prepared it.

e. An integral part of terminal security is a **workable, accurate cargo location**

system. Delays in, or confusion over, removing cargo from storage increases the risk of theft or pilferage. Among other things, a good locator system does not give cargo handlers the excuse to wander all over the terminal when looking for a shipment.

f. Devise procedures to **minimize terminal congestion and poor housekeeping,** which result in obstructed visibility of cargo, misplaced cargo, less efficient checking and handling, and other situations promoting theft and pilferage.

States one highly knowledgeable source, "The real enemy of security is congestion. When goods pile up, you lose control, no matter what procedures are in effect." Many carriers try to combat this by discouraging consignees from delaying pickup or acceptance of cargo.

g. If strikes hit other modes or carriers, some terminals should have emergency plans by which to handle in an orderly fashion the anticipated extra flow of cargo (such as through a pickup and delivery appointment system for shippers and consignees).

h. In areas where the rate of truck hijackings is high, a police official suggests that at each delivery point drivers note the indicated mileage, leaving a record at the dock in their logs. If the truck is hijacked, the difference between the mileage recorded at the last delivery and the indicated mileage at the point of recovery-combined with other driver-supplied information—will assist police in pinpointing the drop or fence.

i. Advertise your security efforts in high-theft locations.

I-6 Security Precautions

a. Know employees on all shifts.

b. Do not advertise on trucks, such as "Smoke Brand X-distributed by...."

c. Run radio and TV spots indicating the convenience and other advantages (such as service) of buying through regular channels.

d. Request truck rental companies to post signs warning users that the rental agent is cooperating in theft prevention.

e. Conceal or seal in a pouch the papers covering a load.

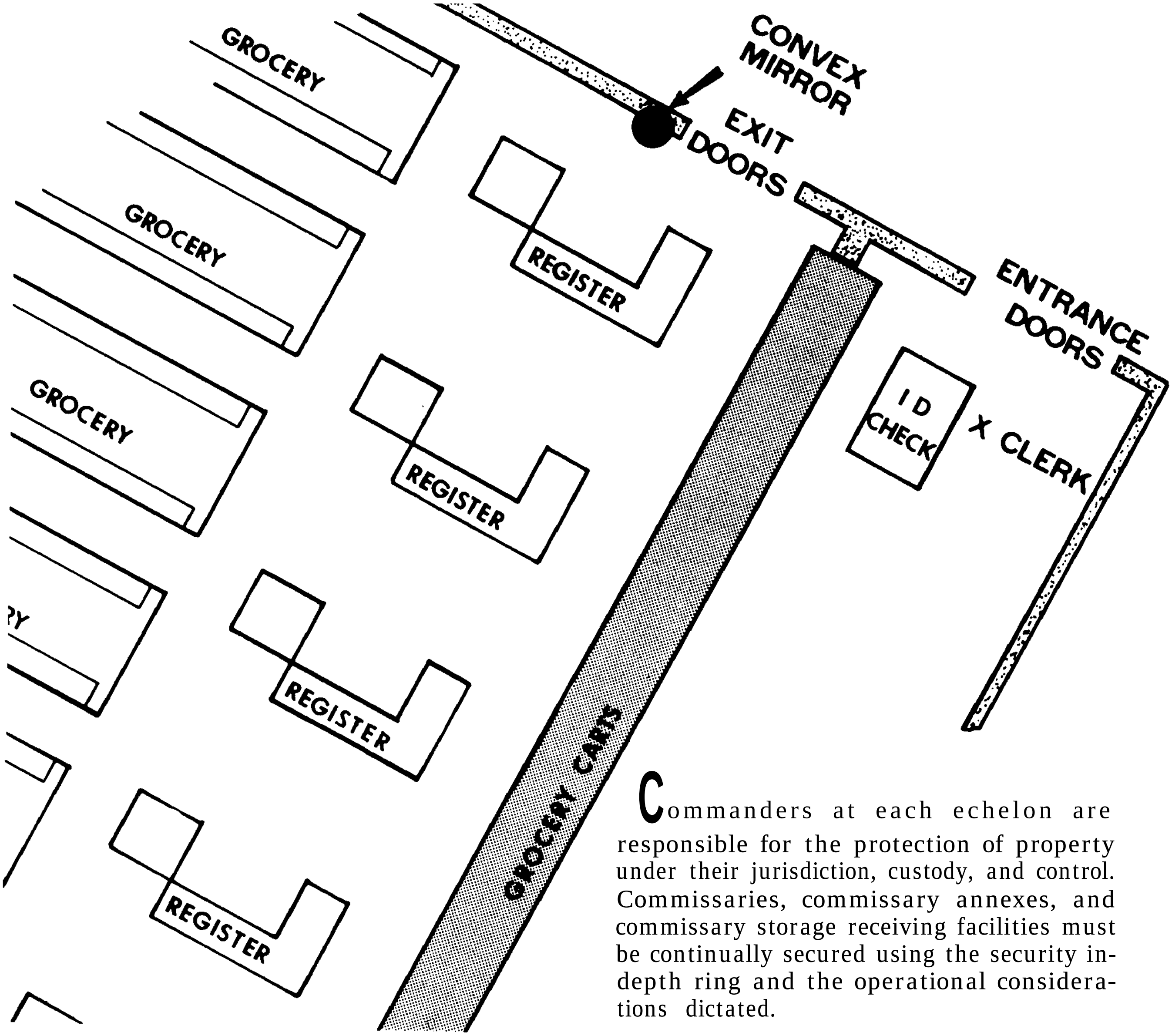
f. Provide cargo checks with self-inking identification stamps. When receipting for cargo, in addition to affixing his signature on the receipt, the checker stamps the document, thereby clearly identifying himself.

g. Use color-coded vehicle passes (keyed to specific areas in the terminal) and time stamp them.

h. Establish advance-notice procedures whereby consignee is notified at least 24 hours prior to arrival of sensitive shipments. Alert intermediate points as well.

Appendix J

Commissary Outlets and Storage



Commanders at each echelon are responsible for the protection of property under their jurisdiction, custody, and control. Commissaries, commissary annexes, and commissary storage receiving facilities must be continually secured using the security in-depth ring and the operational considerations dictated.

Physical protection of commissary and commissary related facilities encompasses measures designed to develop habits and attitudes in commissary employees and supervisors that will emphasize security through:

- Foodstuff protection.
- Providing a secure environment.
- Eliminating potential security weaknesses.

J-1 Controlled Areas

a. Establishing controlled areas for the security of food items will improve the total security posture of the commissary and related facilities by providing security in-depth and insuring that all personnel are security conscious.

b. Although an increase in security measures may cause some slowdown in operation and may inconvenience some personnel, the use of controlled areas assists in identifying security requirements with needs as they develop.

c. Controlled areas are those involving:

- Parking area(s) for incoming shipments of food items (rail, motor transport, air).
- On/off loading area to include the direction of travel area to specific points within a warehouse or to sales outlet.
- Surveillance by physical or electronic methods.
- Control of visiting personnel.

J-2 Facility Construction

a. Doors to the facility must be adequately constructed from a security standpoint.

b. Openings (exhaust outlets, etc.) in excess of 96 square inches must be barred, grilled, or covered with chain-link material.

c. Crawlways beneath the facility should be inspected and secured to add to the overall security posture.

d. The facility must be constructed so that access through unhardened material is impossible.

J-3 Service/Facilitv Entrances

a. The service entrance to the commissary and other related activities must be designed so employee supervisory personnel can observe entry and departure as necessary.

b. The entrance should be located far enough from the cash registers to allow for observation in detecting pilferage.

c. Guard rails should be established to channel personnel entering to purchase items to insure passage through the entry control point from the facility entrance.

d. The service entrance to the commissary sales outlet must be secured to allow opening from the inside only.

e. Service doors should remain locked until the precise operating hours and opened only by designated personnel to allow employee entry.

f. Service entrance doors to warehouse facilities must remain locked at all times during loading and unloading operations or remain under close observation when not secured.

g. Exterior door hinge pins must be of the lock-pin variety or welded to prevent their removal.

h. Padlock hasps must be installed to prevent their removal.

J-4 Patrons

a. Procedures must be established to insure positive identification prior to making a purchase.

b. Admission procedures will be posted in a conspicuous location to inform patrons of store requirements.

c. An established policy on verifying checking credibility must be implemented.

d. A sign should be posted to inform patrons of the possible penalties for shoplifting.

J-5 Store Configuration

a. The store will be arranged to lend itself to maximum observation of attempted employee pilferage or patron shoplifting.

b. There should be circular mirrors at strategic points within the shopping area to provide for observation of dead spaces that cannot be viewed by on-duty employees.

c. Aisles used for patrons should be specifically designed to provide maximum flow for dispersal and reduction of shoplifting.

d. Storage bins will be located and designed to provide adequate security for cardboard boxes which provide monetary input when contracted by weight.

J-6 Incoming Items

a. An effective tally-in and tally-out system will be established for checking items and supplies received or shipped against the available shipping documents.

b. Incoming shipping documents will be filed and periodically reviewed and checked.

c. Incoming items should have continual observation during offloading, delivery, accountability, and storage.

J-7 Meat Disposal

a. The property disposal officer or his designated representative will witness the destruction of meat supplies considered unfit for human consumption. The local official veterinarian will inspect and condemn meat supplies that are unfit for human consumption prior to releasing the items to the disposal officer.

b. Reports of surveys must be requested and initiated when it has been determined that certain items are unfit for human consumption through fault or neglect of the commissary officer and/or employees.

c. Fat trimmings not sold to authorized patrons or issued to organizations subsisted on field rations, must be reported to the installation property disposal officer. A secured and accountable process should be established from departure to delivery of fat trimmings to the installation property disposal officer.

J-8 Cash Register Procedures

a. The amount of cash in the change fund for each cash register should not exceed $150.00 (as established by Troop Support Agency).

b. Each cashier should receipt for either the cash register or the change fund.

c. Cash register tapes and cash receipts

will be reconciled and verified by an authorized representative of the commissary officer at the end of each business day.

d. There will be an established amount that personal checks can be cashed for greater than the total purchase price of the items.

e. Government payroll checks will not be cashed at commissary facilities.

f. The commissary employee entrusted with the monies will be escorted to the bank deposit vault by on-duty military police personnel (appendix K).

g. A periodic records check must be made to verify the transfer of overage funds and receipts to the US Treasury Department.

h. Cash register clearing tapes will be properly accounted for, secured, and forwarded to the appropriate troop support agency in DA Form 3292, Summary of Daily Fund Receipts.

i. Procedures will be established to secure and account for the detail cash register receipts at the end of the business day.

J-9 Locks and Keys

a. The commissary officer will control locks and keys to all buildings and entrances.

b. Keys will be issued to only those people designated in writing by the commissary officer.

c. Keys to entrances and exits will be turned in and placed in a key locker or other secured container at the close of each business day.

d. Keys will not be removed from the installation by employees under any circumstances.

e. Keys, locks, and lock cores will be changed periodically in the event of key duplication.

f. Locks will be changed immediately upon loss or theft of keys or commissary sales items.

g. If multiple-use keys exist, access to such keys must be restricted to the commissary officer or his assistant and secured when not in use.

h. When combination locks are used, the manufacturer's serial number will be obliterated.

i. Locks should be rotated and used at another facility after the second rotation.

j. There will be a person designated to secure and account for on-shelf locks that are targeted to be used for rotation purposes.

k. Safe combinations will be restricted to the minimum number of persons necessary.

1. There will be a current list developed that specifies individuals who are knowledgeable of each combination.

Escorting Public Funds



Proper security during fund escort procedures is of utmost importance. Military police must provide the best security and protection possible when escorting funds. This includes the safety of the person being escorted.

K-1 Security Measures

a. Avoid Patterns.

Avoid escorting at the same time.

- ☐ Refrain from using the same route.
- ☐ Vary direction of approach to pickup and delivery points.
- ☐ Avoid use of same entrance/exit to building for pickup and delivery.

b. Security Sweeps.

(1) A security sweep must be made of the area for suspicious personnel, vehicles, or actions prior to picking up courier.

(2) Where possible, another MP security vehicle should sweep the area prior to arrival of the security escort vehicle.

(3) Check of delivery point by another security patrol prior to arrival of the escort vehicle for suspicious personnel, vehicles, or activities is necessary.

(4) When it is not feasible to use the second security vehicle to sweep the destination point, then the escort vehicle should conduct a sweep of the area prior to delivery.

K-2 Escorts

a. Vehicle Escorts (figure K-1).

(1) Two vehicles should be used for security during the escort of finds.

(2) One vehicle will contain the courier, funds, and an armed MP escort.

(3) The security escort vehicle will be an armed MP vehicle.

(4) MP security personnel will be trained in escort procedures to include being knowledgeable of the predesignated routes.

(5) Vehicle 1 conducts the initial security sweep of route and receiving point while enroute to deposit the payload. Mission permitting, vehicle 1 should cruise the area or establish static surveillance near the deposit facility (bank, etc.) until vehicle 2 has accomplished its mission.

b. Communications.

(1) Security procedures will be established to insure constant communication between escorted vehicle(s) and the MP station.

(2) Establishment of radio security check-

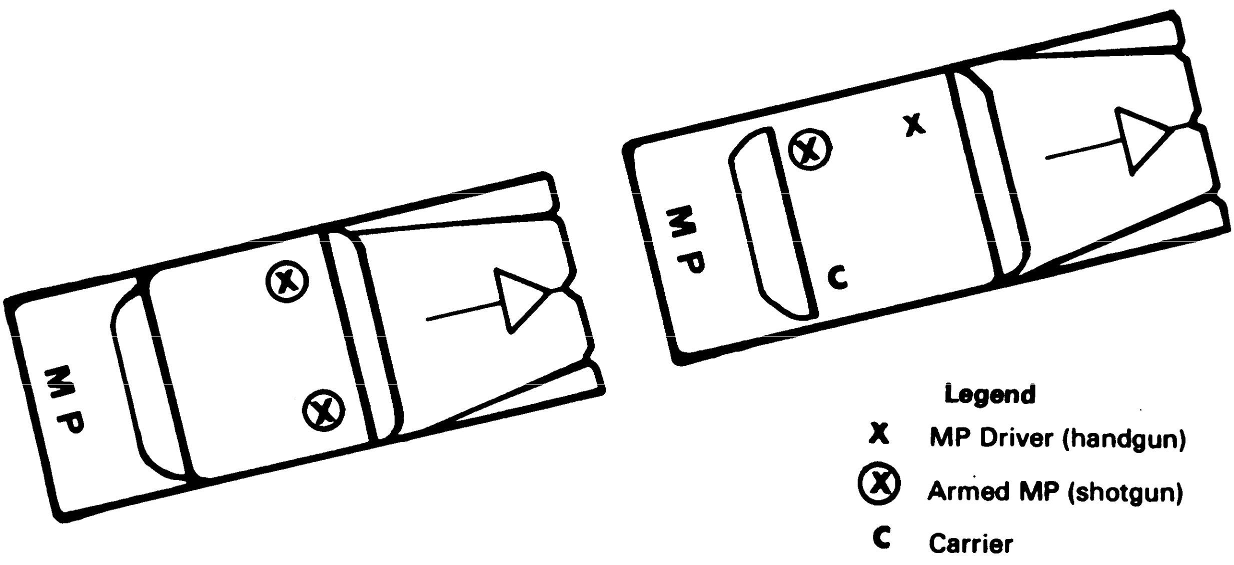


Figure K-1—Placement of occupants in escort vehicles.

points for position identification during movement is essential. Escort status should be relayed to the MP station upon reaching each checkpoint.

(3) Procedures for duress must be estab lished while in a mobile posture and while on foot from patrol vehicle to the depository. As an example of a duress code, the Julian date on the calendar could be used as well as the remaining days of the calendar year.

(4) All escort personnel must have portable radio communications capability while separated from the escort vehicle.

K-3 Protective Actions

a. Protective Cover.

(1) Preselected safety positions should be identified to use if a robbery is attempted.

(2) The motor vehicle, if properly positioned, will provide adequate cover during small arms fire.

(3) A member of the escort team will provide cover of pickup and delivery points from a nearby safe position.

(4) Escort team members will not, except in emergencies, be in possession of fired containers.

b. Response Plan.

- The plan must be designed for responding to holdups, and the military police performing fund security must be briefed on the plan.
- It should provide procedures for cordoning potential holdup areas.
- The response plan should allow for installation closing in case of holdups.

c. Coordination.

- Coordinating the pickup and delivery time of courier personnel will reduce complacency.
- Coordinate with the fund facility manager to obtain the name, information, and pictures of courier personnel to assist identification and to expedite escort procedures at pickup points.
- Request employees working at the pickup and delivery points to observe escort arrivals and departures while maintaining telephonic contact with the MP station.
- Brief courier personnel to possible courses of actions in case of a holdup while on foot, or positioned in vehicle.
- Positive identification of escort personnel to courier must be made prior to arrival and by courier upon arrival.
- Consolidation of fund escort schedules should be accomplished to the maximum extent possible.
- In oversea areas, coordinate with local national police in reference to nation-to-nation agreements on escorts, use of firearms, and carrying of weapons.

d. Backup Response Forces.

(1) Readily available, armed, and equipped.

(2) Trained in small unit tactics.

e. Compliance.

- AR 190-28.
- Traffic regulations.
- Instructions by civil police escorts while off post, providing there is violation of federal law, or lessening the protection of funds.
- Emergency equipment procedural use.

f. Training should include the following:

(1) Threat potential.

(2) Use of force.

(3) Small unit tactics.

(4) Limited crisis intervention counseling.

(5) Escort procedures.

(6) Weapons firing.

(7) limited, low-speed pursuit operations.

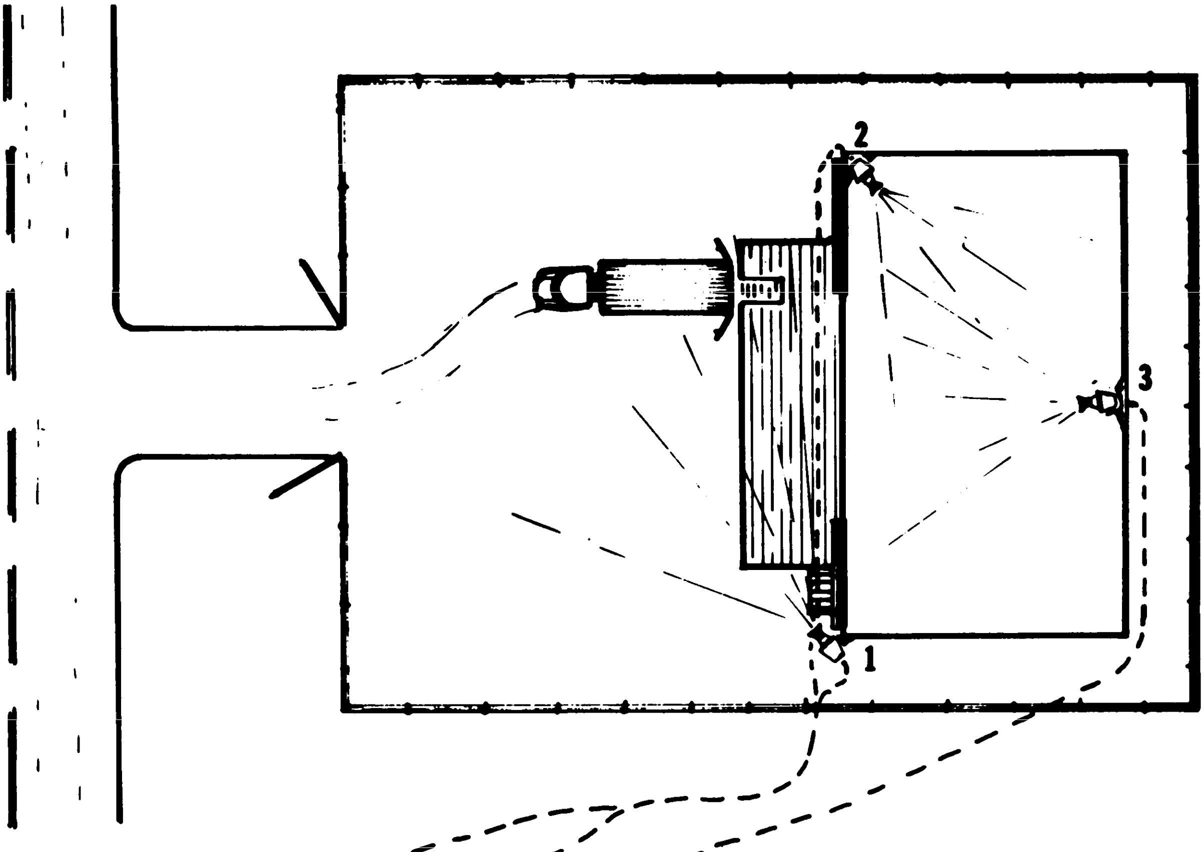
(8) Advanced driver training techniques (TC 19-17).

(9)) After-action reports of previous hold-ups on military installations in various geographical locations.

Note: Funds of less than $500 should be escorted by the responsible fund activity, depending upon the threat posture. All funds involving post exchange, commissaries, clubs, etc., will be escorted by an MP armed guard.

Appendix L

Closed Circuit Television





In security, closed circuit television (CCTV) is designed for a limited audience- the security manager and/or a few guard force members. It is used in some military consumer outlets to prevent and detect pilferage and is used at various guard sites, warehouses, and docks in the remote mode. A CCTV system can be installed in any building or outdoor area in the interest of security if electricity is available.

For the security manager to be effective in selecting and employing CCTV, it is essential that he become knowledgeable of component parts, camera movement capability, and types of shots.

L-1 Characteristics

a. The camera can operate under any marginal light conditions and provide adequate security surveillance of the low-light-level type.

b. Provides continuous operation and is advantageous in that it eliminates delay time required for camera to warm up and be properly adjusted.

c. Adjustment of the TV is critical, especially when enclosed in metal facilities to provide essential security.

L-2 Component Parts

The following components make up a CCTV system:

- Television camera
- Automatic zoom lens
- Manual controls
- Mounting equipment.

L-3 Camera Movement

To detect pilferage, theft, or intruders in all directions (360 degrees), the camera should be able to:

(1) Pan-turn horizontally, left to right, or right to left.

(2) Tilt-aim the camera up or down.

(3) Zoom-change the camera's field of view from wide-angle to close up while the camera is in a stationary position (through automatic changing of the focal length of the lens).

L-4 Operation

CCTV operation capability should include the following:

- Operate by remote control by security personnel at guard headquarters.
- The camera can provide routine and continuous monitoring of activity.
- Preplanned monitor and automatic zoom of activity at specified time intervals.

L-5 Control Room

The control room is located at the guard headquarters in case of dispatching of guard force members.

a. Control room monitor equipment is connected by cable to remote cameras (multiple) conducting security surveillance.

b. Security personnel will occupy control room according to established policy.

c. The control room must be well secured at all times with limited access.

d. The system should have a pushbutton capability to randomly select different operational areas for monitoring, depending upon shipping, receiving, and potential intrusion interests.

L-6 Shot Classification

The following types of camera shots should be available for security consideration (see figure L-1):

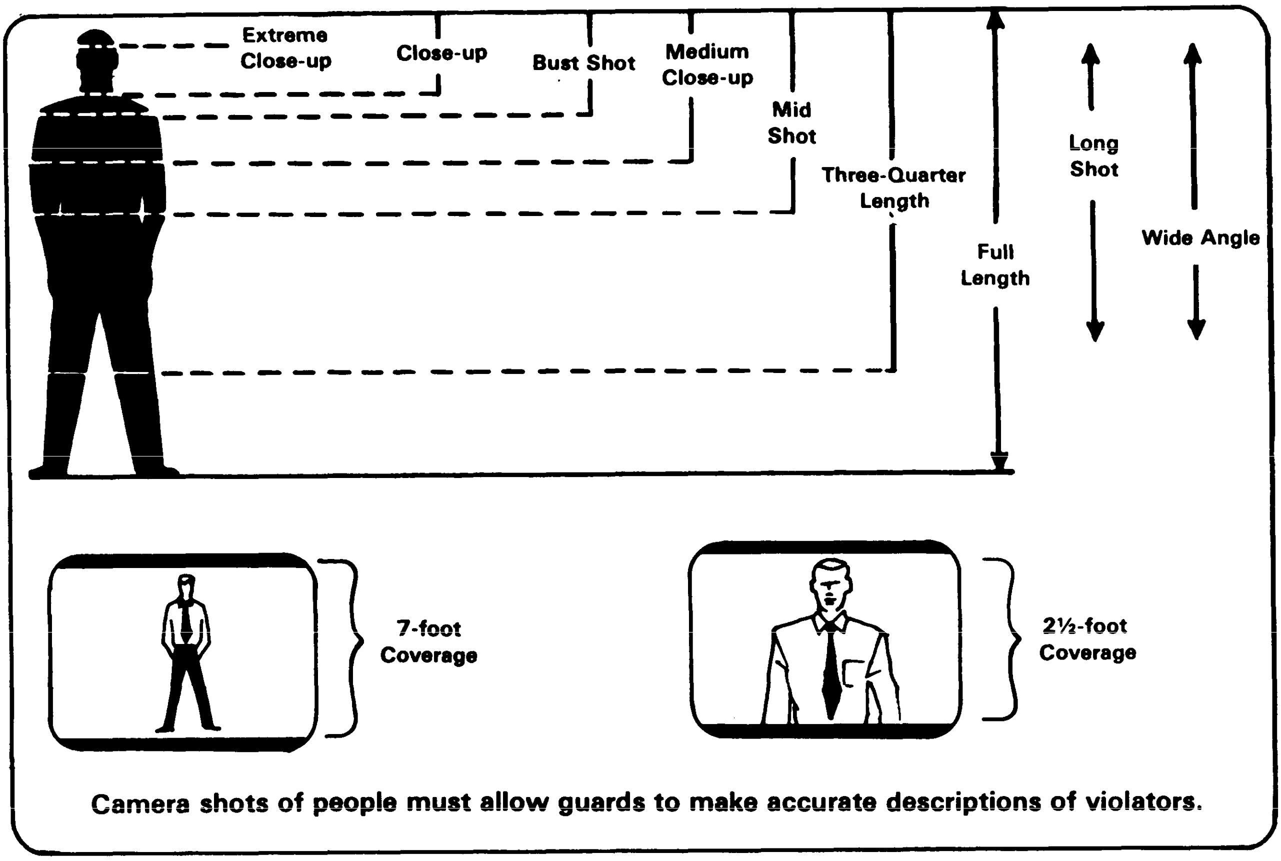


Figure L-1—Camera shot classifications (lens lengths).

- Extreme closeup
- Closeup
- Bust shot
- Medium closeup
- Midshot
- Three-quarter length
- Full length
- Long shot
- Wide angle.

L-7 Employment

Use of a CCTV system at entry/exit control points should meet these guidelines:

(1) Includes a two-way communication system.

(2) Used between the monitor panel and the control points.

(3) Where electrically operated gate locks are used without guards.

(4) The system should allow an individual at the monitor panel to converse with the person desiring entry.

(5) The camera should show a person on the monitor so that authority to enter can be determined.

(6) The gate lock can be remotely released to allow entry when authorization is verified.

(7) Allows observation of security cages, high value goods in warehouses, fence lines, parking lots, banks, ports, ships, etc.

Note: Adaptation to CCTV equipment can allow monitor personnel to make side by-side comparison of an individual's face with the picture on an identification card. Also, an area can be observed through zones (figure L-2).

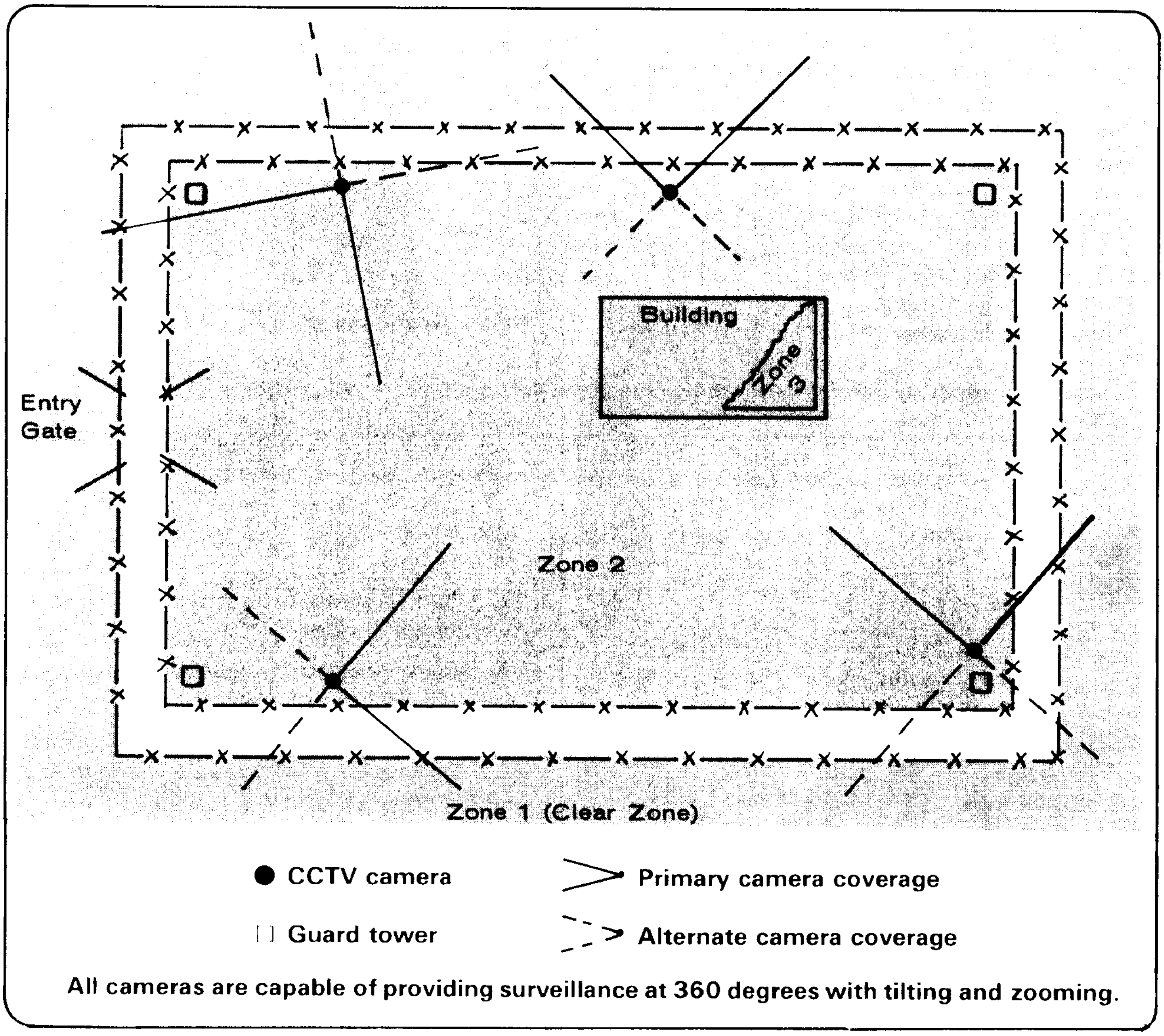
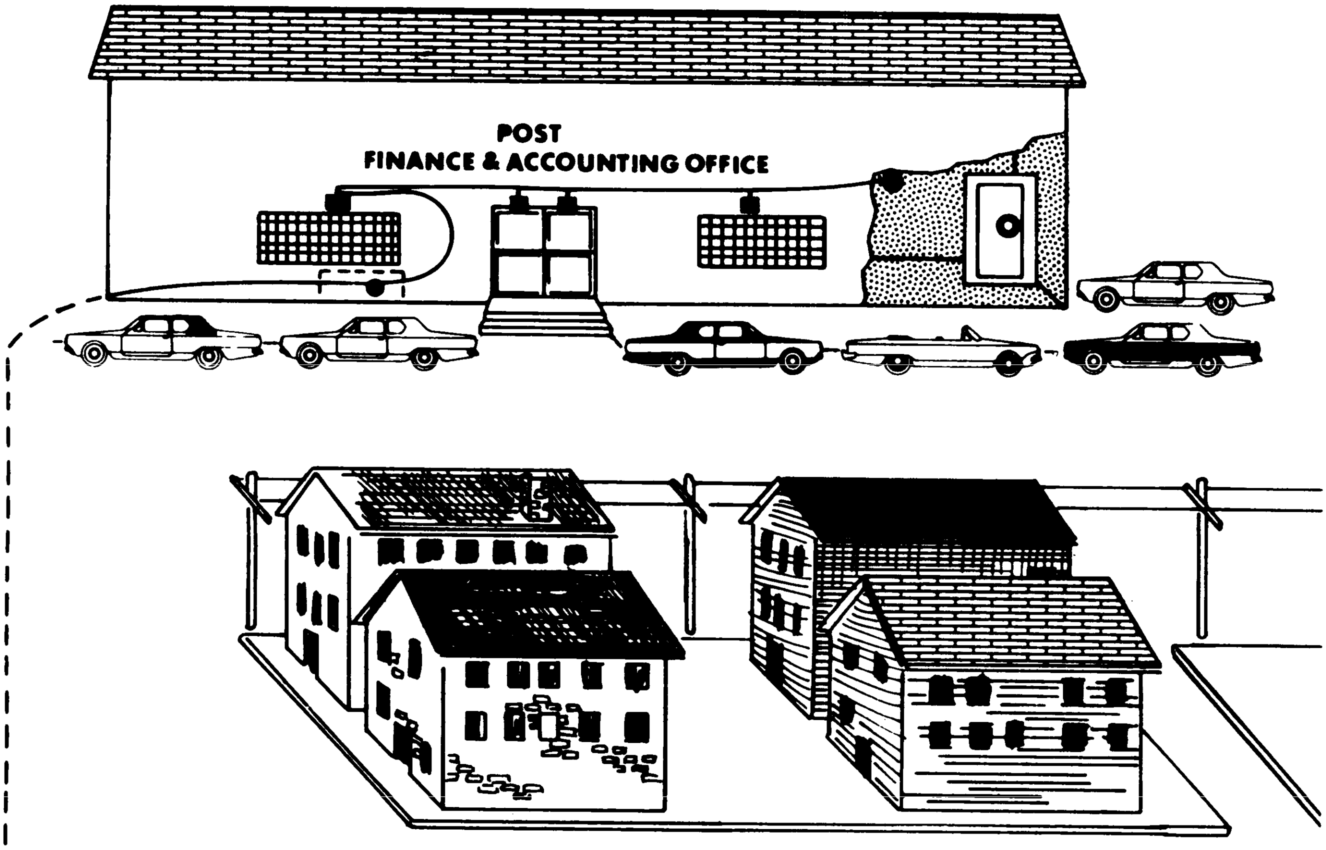


Figure L-2—Example of zone observation by CCTV cameras.

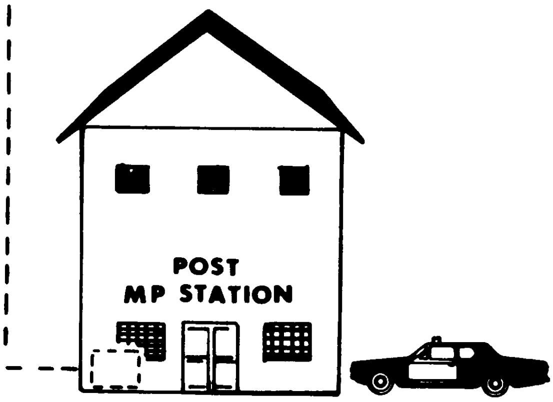
Appendix M

Finance and Accounting Office



Security of finance and accounting offices must be very detailed concerning:

- Vaults
- Cash, controls
- Cashiers
- Agents, checks, and bonds
- Locks, keys, and combinations.



The following questions concern the operation of your finance and accounting office and should be answerable in the affirmative. They are guidelines to assist you in determining adequacy of security. These questions are not all-inclusive. Reference to applicable AR 37-103 and other directives is essential to insure a comprehensive security program for your finance and accounting office (FAO also can mean finance and accounting officer).

M-1 Overview

a. Are there adequate facilities for storing and safeguarding public finds and documents?

(1) Do railings or counters exist to prevent unauthorized entry to the working areas?

(2) Are windows used for exchange of money constructed to prevent individuals outside the windows from reaching funds inside?

(3) Are entry controls to vaults and safes adequate and stringently enforced?

(4) Are the combinations of vaults and safes changed at least every six months and upon the departure/transfer of personnel with knowledge of the combinations?

b. Are procedures established to provide two disinterested individuals to witness the opening of either the cashier's or FAO's safe when the FAO or cashier are not present?

(1) Is there a requirement for disinterested persons to sign affidavits as to the contents of the safe at the time of opening?

(2) When vaults or safes are opened, does the person using the combination protect the dial from observation?

M-2 Cash Controls

These questions cover general considerations for cash control:

a. Is an amount in excess of current disbursing needs promptly deposited to the credit of the Treasurer of the United States?

b. During temporary absence of a clerk(s), is either a drawer with a key lock, or field/similar safe, provided for safeguarding funds and vouchers?

c. If possession of funds is allowed for moral than one employee, is each individual provided a separate and secure receptacle for these monies?

d. Is there a procedure for unannounced verification of cash on hand? Do current records indicate that these verifications are being made on a quarterly basis?

e. Has authority to keep a specific amount of cash on hand been approved by the major command?

M-3 Cashier(s)

- Is each provided with a separate working space?
- Is there a properly enclosed cage or room with a window for paying and receiving?
- Is positive identification of the payee made prior to each cash payment?
- Is each provided a list of AWOL personnel, soldiers reported as receiving several casual payments, and imposters seeking entitlements to authorized individuals?
- Is each furnished a current list of lost or stolen personal financial records (PFR)? (changed in 1971)
- Are receipts taken for all entrusted funds?
- Are receipts given for all funds returned or valid vouchers accepted?
- Is a detailed record maintained of daily settlement with the disbursing officer (or the deputy)?
- If a weapon is furnished, is the cashier qualified in its use? (Arming is not mandatory.)

M-4 Class A Agents

- Instructed in writing on their duties and responsibilities? (Required by AR 37-103.)
- Promptly account for finds?

M-5 Blank Checks And Savings Bonds

a. Initial Delivery to FAO.

(1) Upon receipt of shipments, are the cartons examined and the serial numbers checked?

(2) Are cartons bearing evidence of tampering, opened, and checks counted individually?

b. In Current Use.

(1) Prior to use, are they kept under lock and key in the safe of the FAO (or the deputy)?

(2) Does the FAO (or deputy) inspect blank checks and bonds at the start and end of each day's business to determine if any have been extracted?

(3) Does the FAO (or the deputy) maintain a daily record of the number released, written, and returned for safekeeping?

(4) When voided or spoiled, are they properly marked and reported? Are such items properly safeguarded?

(5) Are there proper controls for mailing and/or delivering checks and savings bonds to prevent loss?

(a) Are internal office procedures established to provide controls on all undelivered and returned checks and savings bonds?

(b) Is there a central point for their receipt, holding, and final disposition?

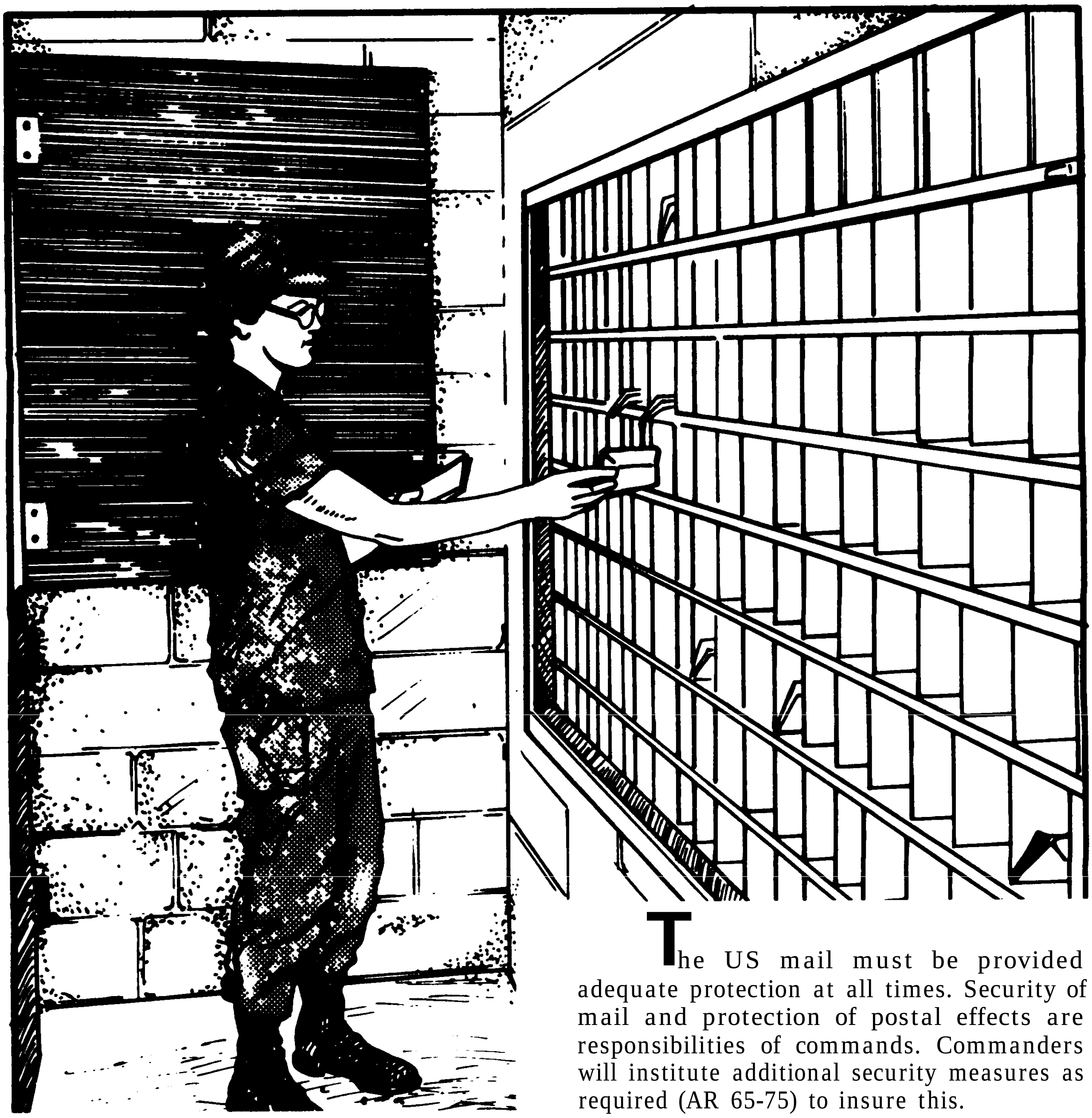
(c) Is responsibility charged to a specific individual?

M-6 Locks, Keys, And Combinations

- ❑ Are ke ys to the locking devices of the meter and protection unit of check signing machines kept in the custody of the FAO (or deputy) at all times?
- ❑ Does the FAO (or deputy) keep a current list published of personnel authorized keys to the office?
- ❑ Is the cashier the only person with keys and combinations to the cashier's safe and cash drawer?
- ❑ Has the cashier sealed one key to and/or the combination of the safe in an envelope?
- ❑ Has he or she suitably marked the envelope so that its unauthorized opening maybe detected?
- ❑ Is the envelope secured in the safe of the FAO?
- ❑ Is the combination to the FAO's vault or safe known only by the FAO?
- ❑ Has a copy of the combination been sealed in an envelope suitably marked to detect unauthorized openings **and placed in the possession of the installation commander for use in an emergency?** Is the envelope marked to reflect that it will be opened only in emergencies and with specific consent of the installation commander, his alternate or equivalent of Chief of Staff; and that two disinterested officers will inventory and witness the contents of the vault safe?

Appendix N

Mail and Postal Effects



The US mail must be provided adequate protection at all times. Security of mail and protection of postal effects are responsibilities of commands. Commanders will institute additional security measures as required (AR 65-75) to insure this.

The following questions concern the mailroom. If you can answer "Yes" to all questions, you can be confident that your security is adequate. These questions are not all-inclusive. Reference to applicable Army regulations and other directives is essential to insure a comprehensive security program.

N-1 Responsibility

Are personnel appointed by the unit commander?

- ■ Unit mail supervisor— **in writing?**
- ■ During periods of temporary absence (such as leave, pass, TDY, hospitalization, etc.), alternate unit mail supervisor, **in writing?**
- ■ Mail clerk? Alternate mail clerk, at least one?

N-2 Design Construction

- ☐ Separate room?
- ☐ Reinforcement for walls and ceilings of soft materials?
- ☐ Protection of door?
  - ☐ Hinges and hasps mounted to decrease the possibility of removal? Spot-welded or peened-hinge pins, if hinges on outside of door.
  - ☐ Equipped with one or more secondary padlocks?
- ☐ Protection of openings permitting entry?
  - ☐ Adjoining room doors, trapdoors, etc., locked and/or blocked?
  - ☐ Windows, ventilation, etc., covered with steel bars or screened with heavy wire mesh?
  - ☐ Wire mesh anchored to preclude unauthorized removal?
  - ☐ Field safe or other suitable container provided for registered and/or certified mail?
  - ☐ Affixed to the structure to sigificantly decrease possibility of removal?
  - ☐ Meet the requirements of AR 380-5 for overnight storage of official registered and/or certified mail?

N-3 Operation

a. Used exclusively for mail activities?

b. Exterior posting of provisions of entry signs?

c. Entry list of authorized personnel kept current and signed by the unit commander or unit mail supervisor.

d. Items of mail kept out of the reach of individuals standing outside the mailroom door?

e. Transportation of mail to and from the post office is:

(1) In a closed-body vehicle equipped with a rear door?

(2) If not does the mail clerk ride in the compartment of the vehicle containing the mail?

f. Delivery to only the addressee or agent designated in writing by the addressee?

g. Positive identification required of an individual addressee agent before delivery of registered, number insured, or certified mail?

h. Are there written instructions on required actions for known or suspected postal offenses, such as willful destruction, loss, theft, delay, etc., of mail?

N-4 Locks, Keys, And Combinations

Does the mail clerk or alternate have one set of keys in their possession at all times to locked mail receptacles, such as mailroom, mailboxes, safes, individual lockboxes, etc.?

Are all copies of each combination and/or duplicate keys individually sealed in separate envelopes?

- ☐ Do the envelopes indicate the contents?
- ☐ Have the unit commander or mail supervisor and the mail clerk written their names across the sealed portion of each envelope? (This procedure assists in detection of tampering.)

Is there a requirement for the prompt change of combinations and/or keys and locks to the mailroom and all mail receptacles upon the transfer or the AWOL of the mailclerk(s) and/or unit mail officer?

Use of individual lockboxes:

- Does only one individual have overall authority and responsibility for issuing and changing the combinations and/or keys and locks?
- Is there prompt change of combinations and/or keys and locks upon transfer of personnel to whom boxes were assigned?

Is there a prohibition in effect against the use of master keys and/or **"SET"** locks for the mailroom and mail receptacles?

N-5 Mailboxes

a. Do they provide protection for all deposited mail from weather and other natural or human security threats? (see figure N-1 for sample.)

b. Construction:

(1) Built into fixed foundation(s)?

(2) Adequate size and depth to protect quantity of mail accumulated over weekends/holidays?

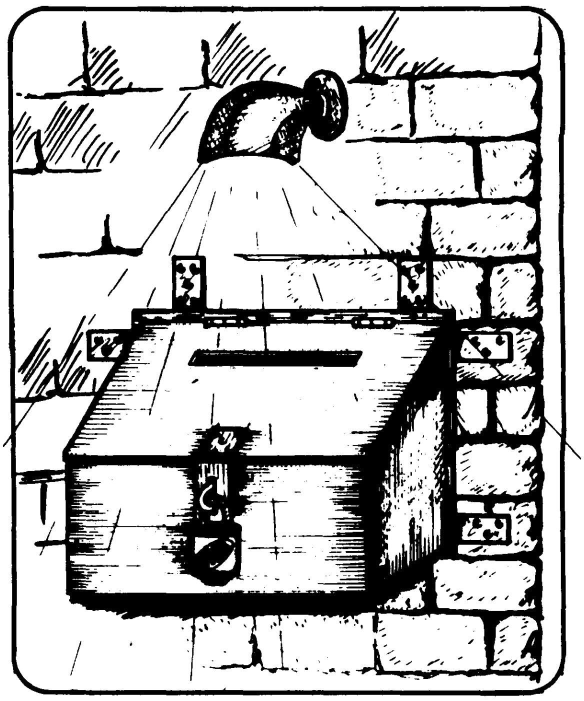


Figure N-1—Example of properly secured interior mailbox.

The following questions concern minimal general security requirements.

N-6 Security

- Does the facility provide security against unauthorized entry?
- Do the doors have proper locks?
- Are all windows barred or covered with heavy wire mesh?
- Are walls and ceilings of material suitable to prevent forcible entry?
- Was particular attention given to the procurement of safes?
- Is particular attention provided to use of the safes?
- What about the attention provided to other receptacles?
- Is registered mailroom adequately secured, and is log of all entering personnel maintained?
- Are off-duty postal personnel denied entry?

N-7 Accountable Items

a. Is there adequate security afforded blank money orders, money order validation plates, postage stamp stock funds, and fund effects?

b. When a vault is not available, are accountable items secured in a cash box and delivered to the custodian of postal effects (COPE) or designated NCO for safekeeping?

c. Is the yearly record of unit mailroom inspections, DA Form 4216-R, properly maintained and on file for review?

d. Are mail vehicles properly closed and sealed before dispatch and properly unsealed on arrival at destination?

e. Are there proper controls by the designated seal control officer for numbered seals employed?

N-8 Emergencies

a. During emergencies (fire, flood, burglary, or other forced entry, etc.), are security guards required to be posted?

b. Have arrangements been established for security personnel to safeguard mail, postal effects, equipment, and property for as long as needed by investigative authorities?

N-9 Safes

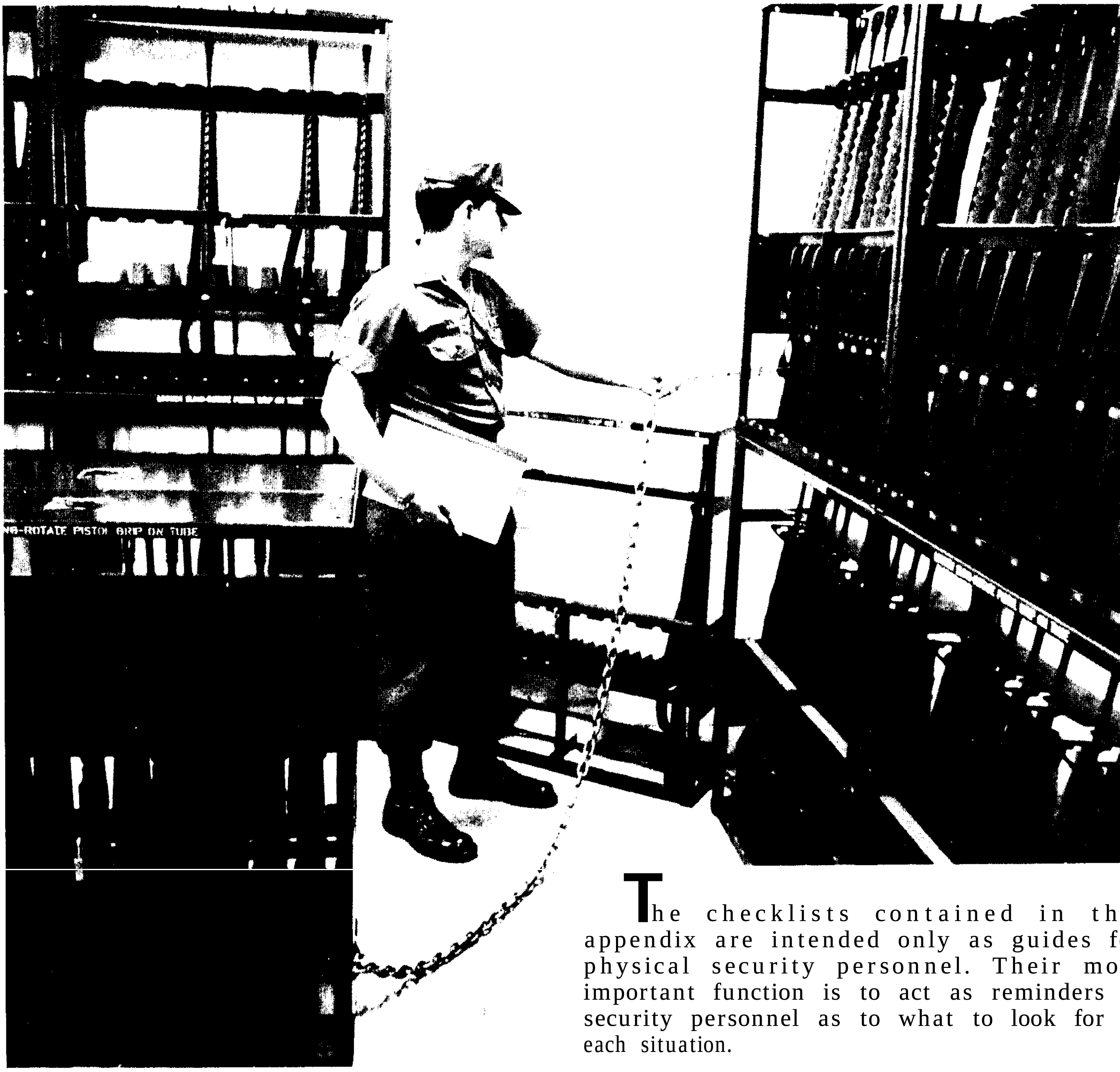
Are authorized safes secured to prevent removal?

Are proper security checks of safes conducted during opening and closing procedures?

Have specific persons been designated to open the safes?

Appendix O

Checklists



The checklists contained in this appendix are intended only as guides for physical security personnel. Their most important function is to act as reminders to security personnel as to what to look for in each situation.

These checklists must not be viewed as complete or all-encompassing. In individual situations, there may be items of physical security interest and importance which are not included on any of the checklists. Security personnel must be alert for such items, and not be content merely to check off the items on the checklist.

For some facilities or installations, none of the checklists will specifically apply. In such cases, security personnel should formulate their own checklists, using any of the items on the attached lists as basic guidance and adding any items peculiar to the facility or installation.

There also will be situations in which more than one of these checklists will be useful. This may occur where more than one of the activities covered by the checklists is housed in a single building.

No specific sources of reference are provided for the individual items on these checklists. Such specific references rapidly become outdated as Army regulations, field manuals, and their publications are revised and republished. Also, many such references are supplemented by command publications which impose changed or additional requirements.

These checklists may also be adapted to the style of a locally produced form, with appropriate heading, general information spaces, and columnar headings with boxes for “yes,” “no,” and/or similar checks. DA Form 2806 is an example of such a form.

Waiver/Exception

1. Has a waiver/exception been granted for specific requirements of AR 190-11? ☐ Yes ☐ No

2. If the waiver was granted, is it valid? ☐ Yes ☐ No

3. Are the specific requirements set forth in the granted waiver/exception being complied with? ☐ Yes ☐ No

4. Are compensatory measures on which the wa iver/exception is based in effect and are they appropriate to provide sufficient security to insure reasonable protection for the property contained in the storage facility? ☐ Yes ☐ No

5. Are the required enclosures attached to the granted waiver/exception as outlined under the provisions of AR 190-11? ☐ Yes ☐ No

6. What is the issue date of the waiver/exception? ______________

Arms Storage Building

1. Is the building used to secure only small arms? ☐ Yes ☐ No

2. Are the walls constructed of 8 inches of concrete, reinforced with No. 4 bars at 9 inches on center in each direction and staggered on each face to form a grid approximately 4½ inches square? ☐ Yes ☐ No

3. Are the walls constructed of 8-inch concrete blocks with No. 4 bars threaded through block cavities at 8-inch centers with the cavities then filled with mortar or concrete and with horizontal joints reinforced at every course? ☐ Yes ☐ No

4. Are roof structures and/or ceilings of fire resistant construction to provide an equal or greater degree of security as the approved protection of windows and doors? ☐ Yes ☐ No

5. Are walls constructed of 8 inches of brick interlocked between inner/outer courses? ☐ Yes ☐ No

6. Is the number of doors and windows limited to only the essential? ☐ Yes ☐ No

7. Is the building posted as a restricted area? ☐ Yes ☐ No

8. Are all windows protected by rod and bar grid/steel bars horizontal at 8 inches maximum on center, and ½-inch diameter rods vertical at 4 inches maximum on center welded to, or passing through, the 1¼-inch surface of the flat bars, resulting in a grid with openings of 32 square inches or less? ☐ Yes ☐ No

9. Is each rod and bar grid secured to a steel frame securely attached to the building with fastenings inaccessible from the outside? ☐ Yes ☐ No

10. Are the ends of the steel bars securely embedded in the structure of the building or welded to a steel frame securely fastened to the building with the fastenings inaccessible from the outside? ☐ Yes ☐ No

11. Are all windows locked at the close of the business day? ☐ Yes ☐ No

12. Are all doors constructed of materials that will render access by force extremely difficult? ☐ Yes ☐ No

13. Are all doors, except the main entrance, secured on the inside by locking bars? ☐ Yes ☐ No

14. Are door frames fastened to the building so as to prevent them from being separated from the casing? ☐ Yes ☐ No

15. Is the main entrance door secured by at least one high security padlock? ☐ Yes ☐ No

16. Are outswinging doors mounted on fixed-pin security-type hinges, safety stud hinges, or the equivalent? ☐ Yes ☐ No

17. Is there adequate exterior and interior lighting? ☐ Yes ☐ No

18. Are ceilings constructed of reinforced concrete, structurally designed for the spans between supporting walls with reinforcing bar spacing forming a grid in which the area of any opening does not exceed 96 square inches using No. 4 bars or larger? ☐ Yes ☐ No

> Note: Active Army and USAR consolidated arms storage facilities may use woven wire mesh caging with individual locks on each door in lieu of separate walls between unit arms rooms.

Arms Storage Room

1. Are procedures established and stringently applied to reduce the opportunity for unobserved access to the arms storage room within the building? ❑ Yes ❑ No

2. Do internal procedures include prevention of loitering in close proximity to the arms room, either inside or outside the building? ❑ Yes ❑ No

3. Is the arms room posted as a restricted area? ❑ Yes ❑ No

4. Is the number of windows limited to the essential minimum? ❑ Yes ❑ No

5. Are windows protected with rod and bar grids? ❑ Yes ❑ No

6. Is each rod and-bar grid secured to a steel frame securely attached to the building with the fastenings inaccessible from the outside? ❑ Yes ❑ No

7. Are the ends of the steel bars securely embedded in the structure of the building or welded to a steel frame securely fastened to the building with the fastenings inaccessible from the outside? ❑ Yes ❑ No

8. Are all windows locked at the close of the business day? ❑ Yes ❑ No

9. Does the arms room provide triple barrier protection? ❑ Yes ❑ No

10. Are the doors constructed of steel bars welded to a grid with openings of 32 square inches or less, or a solid wooden door covered on the outside with steel plate(s) of at least 12 gauge? ❑ Yes ❑ No

11. Are door hinges of the fixed-pin security hinge type or of a type that provides equivalent security? ❑ Yes ❑ No

12. Unless safety stud hinges are used preexposed hinge pins spot welded or otherwise secured to prevent removal? ☐ Yes ☐ No

13. Are all doors used for access to the arms room locked with approved locking devices? ☐ Yes ☐ No

14. Is the locking device on the most secure door a high security padlock and hasp? ☐ Yes ☐ No

15. Is there at least one approved locking device on each door of the triple barrier system? ☐ Yes ☐ No

16. If the arms room is equipped with a steel vault type door, does it have a built-in three position, dial-type, changeable combination lock? ☐ Yes ☐ No

17. Are doors not used for access to the arms room of equivalent structural strength as adjacent walls and secured so as to preclude access to the locking device from the outside? ☐ Yes ☐ No

18. If a wire-mesh cage is used for the temporary storage of small arms, is it constructed in conformance with OCE Standard Drawing 40-01-41 and 40-21-01 and kept under continual surveillance? ☐ Yes ☐ No

19. Is a prefabricated cage used to reinforce arms room as an inner liner to provide additional delay to forced entry? ☐ Yes ☐ No

20. If so, is it used only when structural standards for the arms room cannot be met? ☐ Yes ☐ No

21. In temporary buildings, are the exterior walls of the arms room of double wooden-wall thickness (standard stud construction)? ☐ Yes ☐ No

22. In temporary buildings, are the interior walls, ceiling, and floor constructed to insure that at least one side of the surface is 1-inch, double-nail, tongue-and-groove wood sheathing or a material that will provide a similar degree of security? ☐ Yes ☐ No

Arms Racks

1. Are all arms racks or containers locked with approved locking devices when not in use? ❑ Yes ❑ No

2. Are the arms racks fastened together and to the wall or floor with bolts or with approved chains equipped with at least secondary locking devices? ❑ Yes ❑ No

3. Do those racks with hinged locking bars have the hinge pins welded or otherwise secured to prevent easy removal? ❑ Yes ❑ No

4. Do locally fabricated arms racks provide, as a minimum, security equivalent to standard issue racks? ❑ Yes ❑ No

5. Are all racks constructed so that when locked, a weapon cannot be removed by partially disassembling it? ❑ Yes ❑ No

6. Are crew-served and other weapons that will not fit into issue racks secured in containers constructed of at least 22-gauge steel; and if locally fabricated or commercially manufactured, are containers constructed of at least 26-gauge steel? ❑ Yes ❑ No

7. If Class 5 weapons container (map and plan security cabinet) is used by small isolated units having few weapons, is the container adequately augmented by other physical security measures? ❑ Yes ❑ No

8. If lockers are being used as a substitute for racks, are they fastened to the structure? ❑ Yes ❑ No

9. Are hasps of the lockers installed so they cannot be removed? ❑ Yes ❑ No

10. Are lockers equipped with approved locking devices? ❑ Yes ❑ No

11. Are hinges of the lockers installed so they cannot be removed? ❑ Yes ❑ No

Admin Control Procedures

1. Are all weapons' serial numbers entered in unit and/or station property records and kept current at all times? ☐ Yes ☐ No

2. Are all weapons not in bulk storage inventoried by serial number at least once each month? ☐ Yes ☐ No

3. Are written records of weapon inventories accomplished and maintained? ☐ Yes ☐ No

4. Are weapons in bulk storage or in depots properly inventoried and the inventories made into written records? ☐ Yes ☐ No

5. In addition to scheduled weapon inventories, are frequent unscheduled inventories conducted? ☐ Yes ☐ No

6. When more than one unit uses the same arms room or weapons storage facility, are weapons separated and identified by unit? ☐ Yes ☐ No

7. When more than one unit uses the same arms room or weapons storage facility, does each unit maintain individual accountability for its own weapons? ☐ Yes ☐ No

8. Are individuals issued weapons cards? ☐ Yes ☐ No

9. Is the weapons card turned in to the arms room when the weapon is drawn? ☐ Yes ☐ No

10. Do individuals sign a weapons receipt register when weapons are removed from the arms room? ☐ Yes ☐ No

11. Have written procedures been established for issuing weapons and ammunition during emergencies or field exercises, or at other times when operational necessity dictates a need for this equipment to be issued quickly? ☐ Yes ☐ No

→

12. Is the arms or ammunition storage facility checked periodically by a security or guard patrol, or unit personnel? ☐ Yes ☐ No

13. Are all checks recorded? ☐ Yes ☐ No

14. Are individuals who are in possession of weapons or ammunition warned of their responsibilities and the inherent dangers involved in the loss of weapons and ammunition? ☐ Yes ☐ No

Key and Lock Control

1. Are keys to arms storage buildings, rooms, racks, and containers maintained separately from other keys and accessible only to those individuals whose official duties require access to them? ❑ Yes ❑ No

2. Is a current roster of these individuals kept within the unit? ❑ Yes ❑ No

3. Is the number of keys held to the essential minimum? ❑ Yes ❑ No

4. Is the custody of keys transferred between authorized individuals only after both parties have conducted a visual inventory of weapons to include total count of weapons on hand? ❑ Yes ❑ No

5. Is the change of custody of keys properly recorded? ❑ Yes ❑ No

6. After duty hours, are keys locked in a secure receptacle away from the storage area or in the custody of the responsible duty officer/NCO or charge of quarters? ❑ Yes ❑ No

7. Are keys left unattended or unsecured at any time? ❑ Yes ❑ No

8. Is the removal of keys to arms storage buildings, rooms, racks, and/or containers from the installation permitted? ❑ Yes ❑ No

9. Is the use of master keys permitted? ❑ Yes ❑ No

10. Are locks replaced when keys are lost, misplaced, or stolen? ❑ Yes ❑ No

11. Has a key/lock custodian been appointed on orders? ❑ Yes ❑ No

12. Is a key control register maintained at all times to insure administrative accountability for keys? ❑ Yes ❑ No

→

153-846 0 - 94 - 16

13. Does the key control register contain the signature of the individual receiving the key, date/hour of issuance, serial number of key, initials of the person issuing the key, date/hour key was returned and the signature of the individual receiving the returned key? ❑ Yes ❑ No

14. Are padlocks locked to the staple or hasp when the area or container is open? ❑ Yes ❑ No

15. Are inventories of keys and locks conducted quarterly? ❑ Yes ❑ No

16. Are locks and locking devices securing weapons rotated at least annually? ❑ Yes ❑ No

17. Are tools located in the vicinity of the arms storage area secured in a locked container? (See chapter 8, FM 19-30.) ❑ Yes ❑ No

Safeguarding Ammunition And Explosives

1. Is ammunition stored in the unit arms room, authorized by higher headquarters, inventoried daily, and stored and controlled as stipulated by chapter 3, AR 190-11, and safety regulations? ❑ Yes ❑ No

2. Is ammunition assigned on unit property records inventoried monthly? ❑ Yes ❑ No

3. Is a written record made of all ammunition inventories? ❑ Yes ❑ No

4. Is the area where ammunition/explosives are stored posted as a restricted area? ❑ Yes ❑ No

5. When more than one unit uses the same ammunition storage facility, are the stocks separated and identified by unit? ❑ Yes ❑ No

6. Are there written security procedures established which designate one unit responsible for the security of the storage facility? ❑ Yes ❑ No

7. Is ammunition in unit arms room stored in separate locked containers? ❑ Yes ❑ No

8. Is the container firmly secured to the structure? ❑ Yes ❑ No

9. Is the ammunition storage area secured with a high security padlock and hasp? ❑ Yes ❑ No

10. Are ventilators, or other openings affording access to individuals or dangerous objects, equipped with steel mesh or other material offering equivalent protection? ❑ Yes ❑ No

11. Is the control and accountability of keys to ammunition/explosive storage proper? ❑ Yes ❑ No

12. Are locks securing ammunition/explosive storage areas rotated at least annually? ❑ Yes ❑ No

→

13. Is loose ammunition, assigned on the unit property records and not in banded containers, physically counted? ❑ Yes ❑ No

14. Does the monthly inventory of ammunition include an inspection and count of crated ammunition to insure that bands and seals are intact? ❑ Yes ❑ No

15. Does monthly inventory of ammunition in banded containers include lot number(s)? ❑ Yes ❑ No

16. Have agencies or organizations responsible for securing large quantities of ammunition (such as bulk storage in depot, installation ammunition supply points, prestock points) insured that an accurate system of accounting and inventory, such as cyclic inventory, is established and maintained? ❑ Yes ❑ No

17. Does the basic load ammunition storage room meet, to the extent possible, the same requirements as established for small-arms storage rooms? ❑ Yes ❑ No

18. Are all doors secured with approved locking devices? ❑ Yes ❑ No

19. Are fire-control measures and symbols posted? ❑ Yes ❑ No

Privately Owned Weapons

1. Are privately owned weapons and ammunition or authorized war trophy firearms secured in locked containers, separate from military weapons and ammunition in the unit arms room? ❑ Yes ❑ No

2. Is the retention and storage of incendiary devices and explosives permitted? ❑ Yes ❑ No

3. Has a receipt been issued for each privately owned weapon stored in the unit arms room? ❑ Yes ❑ No

4. Is the receipt retained in the arms room when the weapon is in the possession of the individual owner? ❑ Yes ❑ No

5. When the weapon is properly stored in the unit arms room, is the receipt in the possession of the individual owner? ❑ Yes ❑ No

6. Are privately owned weapons withdrawn from the unit arms room only after written approval of the unit commander or his authorized representative? ❑ Yes ❑ No

7. Are applicable state and local laws regarding registration and possession of firearms posted on the unit bulletin board? ❑ Yes ❑ No

8. Are newly arrived personnel briefed on provisions governing possession and use of privately owned weapons? ❑ Yes ❑ No

9. Does the commander conduct unannounced inspections to insure proper storage and control of privately owned weapons? ❑ Yes ❑ No

Loss, Theft, and Recovery Of Weapons, Ammunition, And Explosives

1. How many weapons, if any, have been lost or stolen within the past 12 months? ____________

2. How many lost or stolen weapons, if any, have been recovered during the past 12 months? ____________

3. How many weapons if any, have been the subject of a report of survey during the past 12 months? ____________

4. If a loss, theft, or recovery of weapons, demolitions, or explosives has occurred, was the local provost marshal notified promptly? ❑ Yes ❑ No

Intrusion Detection Systems

1. Are intrusion detection systems installed at permanent small arms storage areas? ❑ Yes ❑ No

2. If not, have these systems been requested by the commander? ❑ Yes ❑ No

3. Has an SOP been published for the operation and maintenance of an intrusion detection system? ❑ Yes ❑ No

4. Does the SOP include:

(a) Instruction for daily testing, activation/deactivation and response? ❑ Yes ❑ No

(b) Requirement that a log be maintained indicating alarm activations by date, time, and type of activation (actual or false)? ❑ Yes ❑ No

5. If the IDS has proven unreliable (excessive false alarms), is the system at fault or is it the result of faulty installation? ❑ Yes ❑ No

6. According to the user's evaluation, is the system adequate? ❑ Yes ❑ No

7. At the time of this inspection, was the system functioning properly? ❑ Yes ❑ No

8. Is the system suitable for its present location and environment? If not, explain in remarks. ❑ Yes ❑ No

9. Is the system capable of accomplishing the job that the responsible using official expects it to accomplish? ❑ Yes ❑ No

10. Does the responsible official user understand that the protective alarm system is designed to detect, not prevent, unlawful intrusion into the protected area or beyond a predetermined point of approach to a protected object? ❑ Yes ❑ No

→

11. Is security of the system provided by the use of physical security measures being built into the system, such as:

(a) Height of reporting lines on poles? ❑ Yes ❑ No

(b) Depth that reporting lines are buried in ground? ❑ Yes ❑ No

(c) Use of shielded transmission and power lines? ❑ Yes ❑ No

(d) Control of access to system equipment? ❑ Yes ❑ No

(e) Use of seals on controls and exposed adjustment mechanisms? ❑ Yes ❑ No

(f) Placement of transmission and power lines inside walls or metal conduit? ❑ Yes ❑ No

12. If local annunciator is used and is displayed on exterior of a building, is it protected from the weather or willful tampering? ❑ Yes ❑ No

13. Is the system underwriter approved? ❑ Yes ❑ No

14. Was the system installed by underwriter-approved service personnel? ❑ Yes ❑ No

15. Is the system equipped with a two-position lock switch for on and off operation? ❑ Yes ❑ No

(a) Are there at least two keys available? ❑ Yes ❑ No

(b) Are adequate key controls exercised? ❑ Yes ❑ No

(c) Can the system be turned on and off from outside? ❑ Yes ❑ No

16. In addition to the on and off switch, is the system equipped with electrical shunt type switches for testing? ❑ Yes ❑ No

17. Is it a multiple purpose system (smoke, water, heat, etc.)? ❑ Yes ❑ No

18. Is the system equipped with a pilot light or with any other type of operational readiness indicator? ❑ Yes ❑ No

19. If an AC power supply is used, is the system designed to operate by automatic switching to DC power when necessary to provide continuous protection? (Standby battery in place?) ❑ Yes ❑ No

20. Is the system designed to make an uninterrupted and silent protective circuit transfer with only a local visible indicator to signal when such transfer occurs? ❑ Yes ❑ No

21. Can activating devices be unobtrusively operated? ❑ Yes ❑ No

22. Are properly cleared personnel used to maintain system? ❑ Yes ❑ No

23. Is the alarm system properly maintained by:

(a) Trained local maintenance personnel? ❑ Yes ❑ No
(b) Readily available trained commercial type maintenance personnel? ❑ Yes ❑ No
(c) An appropriate service contract? ❑ Yes ❑ No

24. Are records kept of all alarm signals received, to include:

(a) Time? ❑ Yes ❑ No
(b) Date? ❑ Yes ❑ No
(c) Location? ❑ Yes ❑ No
(d) Action taken? ❑ Yes ❑ No
(e) Cause for alarm? ❑ Yes ❑ No

25. Is the system tested prior to activating it for nonoperational periods? ❑ Yes ❑ No

26. Are frequent tests conducted to determine the adequacy and promptness of response to alarm signals? ❑ Yes ❑ No

27. Is there any inherent weakness in the system itself? ❑ Yes ❑ No

28. Is it connected to a capable response element? ❑ Yes ❑ No

29. Are activating devices appropriately located and sufficient in number? ❑ Yes ❑ No

30. Is the equipment visible to public view? ❑ Yes ❑ No

31. When system is activated, is it audible on the premises? ❑ Yes ❑ No

32. Are independent transmission lines used? ❑ Yes ❑ No

➛

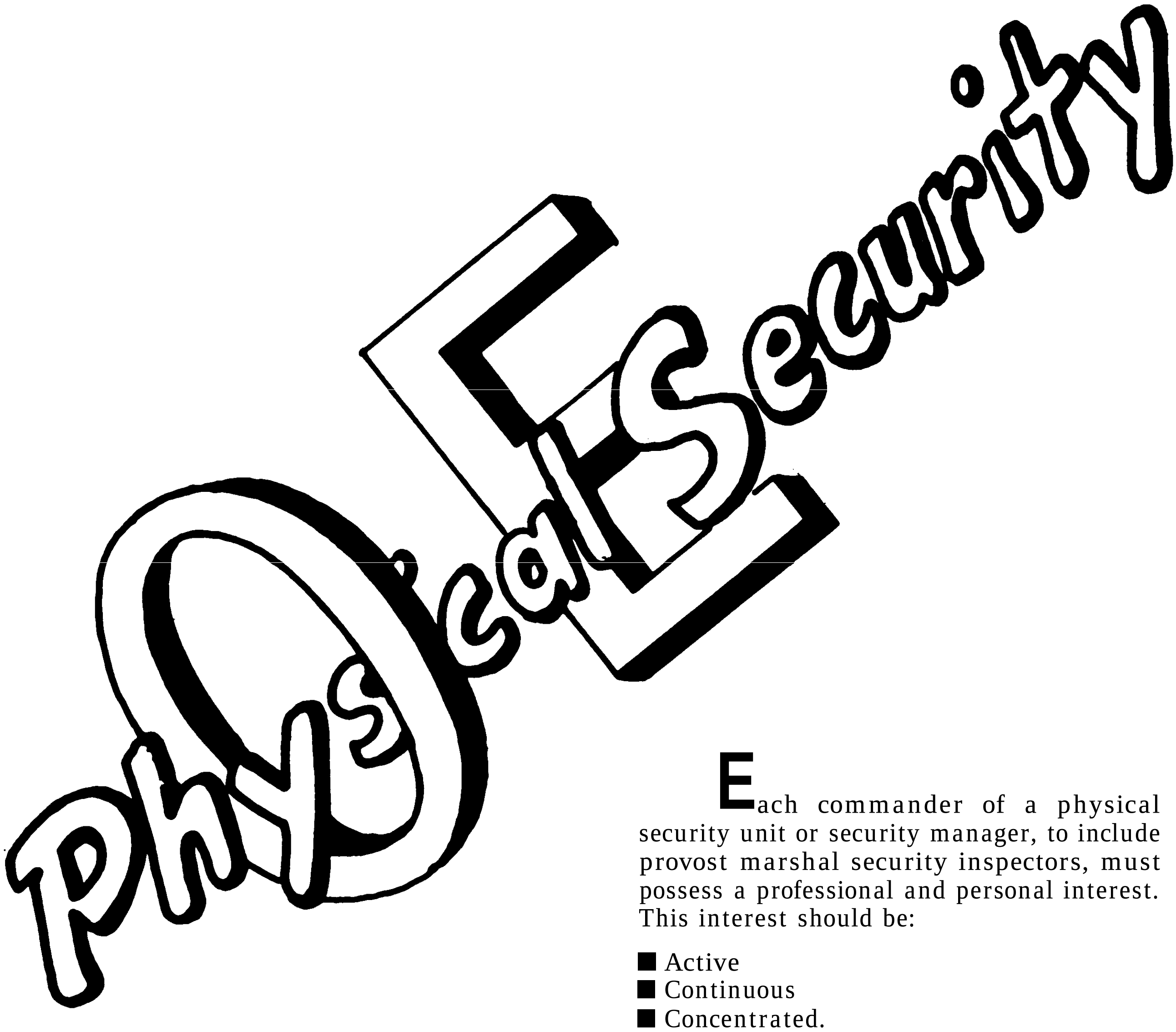
33. Are adequate spare parts, such as fuses and bulbs, readily available to user? ❑ Yes ❑ No

34. Are user personnel capable of conducting minor maintenance and installing fuses and bulbs as required? ❑ Yes ❑ No

35. Is a duress capability built into the system when an authorized person deactivates the system under duress? ❑ Yes ❑ No

Appendix P

Organizational Effectiveness Approach



Each commander of a physical security unit or security manager, to include provost marshal security inspectors, must possess a professional and personal interest. This interest should be:

- Active
- Continuous
- Concentrated.

The psychologically demanding mission of physical security increases the requirement to implement innovative management techniques to reduce the effects of human emotions on unit and other security personnel in performance of their duties. The following psychological factors may impact on human emotions in these conditions:

● ***Isolation—*** assignment to a geographical area which inherently:

- ❑ Limits access to large military communities and facilities.
- ❑ Provides extended observations of desolate areas of land to detect and prevent unauthorized access.

■ ***Disappointment—*** assignment to a security unit and, in some cases, to a security position within the provost marshal's office, as opposed to the traditional "white-hat" assignment, impacts tremendously upon some individuals' morale.

■ ***Frustration—*** evolves due to a lack of prior security educational preparation, of understanding the criticality and importance of the protection of sensitive property to the nation's defense.

■ ***Boredom—*** extended performance of securing (routine tasks within the same operational environment and operating on an individual basis).

P-1 Command Understanding

Individually and collectively all unit personnel must be understood by the command and provost marshal elements to determine security force:

- ■ Capabilities
- ■ Limitations
- ■ Potential.

P-2 Interpersonal Communications

a. Listening, not just hearing.

b. Speaking, not just talking.

c. Establish procedures for unit members to present their creative and constructive ideas to the unit chain of command through:

(1) Unit suggestion boxes.

(2) Rap sessions.

(3) Surveys to determine:

(a) Job satisfaction.
(b) Improvements in security operations.
(c) Adequacy of existing activities and facilities.
(d) Covert drug and other illegal operations within the unit.

(4) The Army's suggestion program.

d. Physical security and inspection personnel must believe that they, as individuals, are important to their unit and section in the total support of its mission.

e. Implementation of the Army's organizational effectiveness process will insure that the accomplishment of the unit and section mission is done in a methodical systems approach.

P-3 Mission Accomplishment

a. The accomplishment of the primary physical security mission when combined with nonsecurity commitments placed

upon the unit and inspector requires the commander and provost marshal to:

(1) Critically assess personnel and equipment resource availability and need.

(2) Assess routine and higher command inspection dates and previous results.

(3) Establish priorities for unit and section goals and objectives.

(4) Establish milestone dates for all goals and objectives identified.

b. To accomplish the security mission, the use of one or a combination of the following management techniques may be used:

(1) Management by objectives (MOB).

(2) Time management (TM).

(3) Decisionmaking.

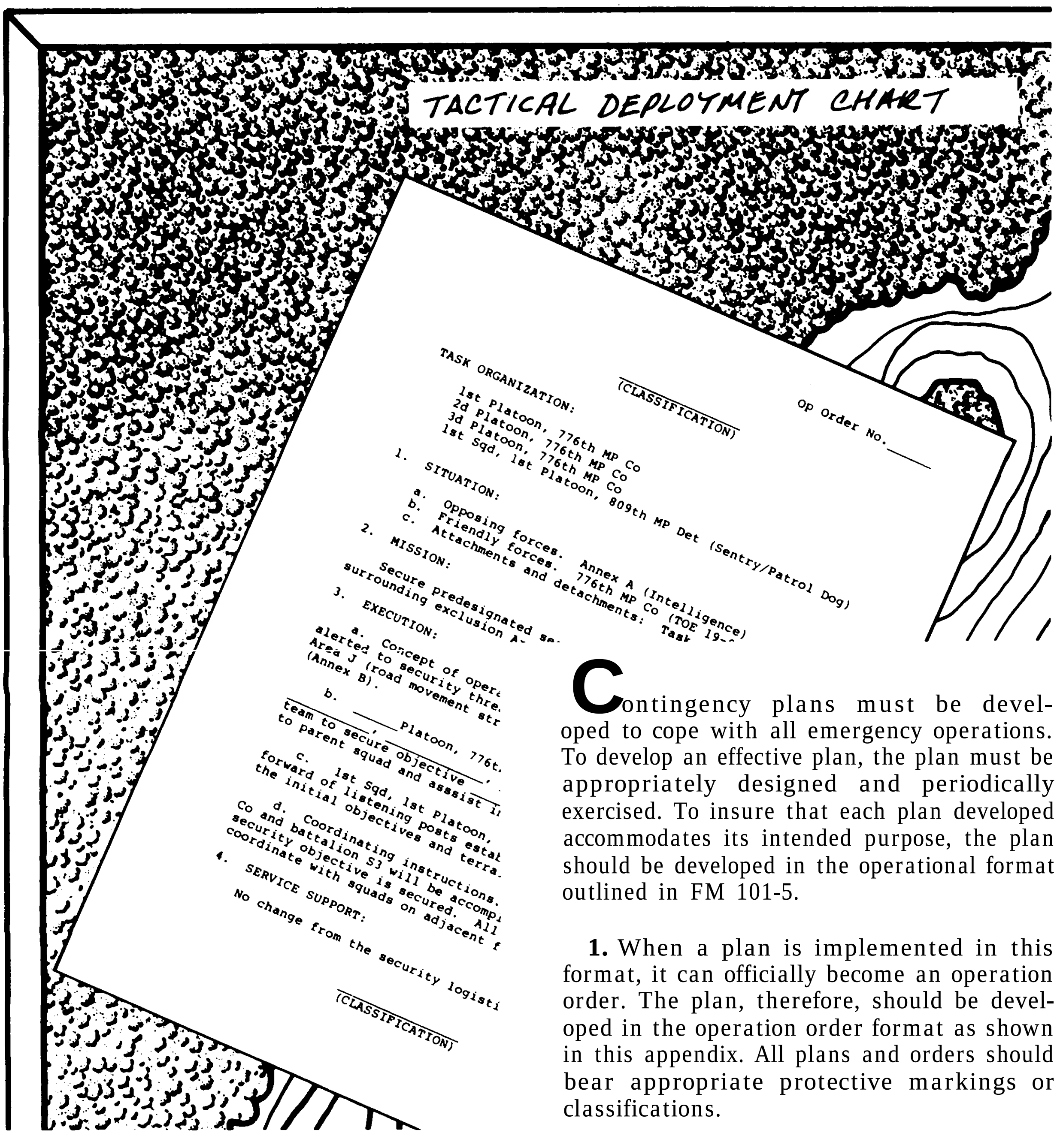
(4) Effective group meetings.

(5) Performance Evaluation Review Techniques (PERT) (modified).

c. Morale and esprit de corps, on and off duty, are achievable goals involving all security matters. The command effort required must emphasize total interpersonal communications.

Appendix Q

Contingency Plans



Contingency plans must be developed to cope with all emergency operations. To develop an effective plan, the plan must be appropriately designed and periodically exercised. To insure that each plan developed accommodates its intended purpose, the plan should be developed in the operational format outlined in FM 101-5.

1. When a plan is implemented in this format, it can officially become an operation order. The plan, therefore, should be developed in the operation order format as shown in this appendix. All plans and orders should bear appropriate protective markings or classifications.

2. The plan/operation order format can be used for various primary and secondary physical security operations. You should have a plan for each of the following, as a minimum:

a. Primary Plans/Operation Orders:

(1) Counter-Terror

(2) Hostage Threat

(3) Bomb Threat

(4) Confrontation Management

(5) Natural Disaster

(6) Nuclear Accident/Incident

(7) Chemical Accident/Incident

(8) Security Alert.

b. Secondary Plans/Operations Orders:

(1) Air Movement Operations

(2) Ground Convoys

(3) Field Storage Movements/Locations

(4) Emergency Escorts.

3. Use the following selected references (not all inclusive) when preparing plans/operational orders for physical security operations:

- AR 190-28, Use of Force by Personnel Engaged in Law Enforcement and Security Duties.
- AR 19-10, Security of Government Officials.
- AR 50-5, Nuclear Surety.
- AR 50-6, Chemical Surety.
- AR 500-50, Civil Disturbances.
- AR 500-60, Disaster Relief.
- AR 500-70, Military Support of Civil Defense.
- FM 31-50, Combat in a Fortified and Builtup Area.
- FM 31-85, Rear Area protection (RAP) Operations.
- FM 3-15, Nuclear Incident/Accident Contaminated Control.
- FM 3-21, Chemical-Biological Contamination and Control.
- FM 19-5, Bomb Threats.
- FM 19-15, Civil Disturbance.
- FM 7-10, Rifle Company, Platoon, Squad.
- TC 19-1, Keeping Your Cool in a Civil Disturbance.

Sample Plan/Order

The sample contingency plan/operational order in this appendix has proven itself in actual use. Its originator also developed the accompanying operational chart to help provide a safe and secure environment for sensitive items. He relates the following experience, which demonstrates how you can develop and implement your own plan.

"One of my first tasks as security manager was to develop a contingency plan to insure the existence of adequate security of the depot. I went to appendix F of FM 101-5 to begin my research. Using my Infantry experience, I developed the plan so that it could be immediately implemented as needed. The plan/order was designed to accommodate an operational order when implemented and to support the unit's specific mission.

"Post Engineers furnished a map of the installation; and I used this for my master tactical deployment chart. I covered the map with acetate and identified the following items:

- ❑ Site location and configuration
- ❑ Key terrain features near the site

- ❑ Security force objectives
- ❑ Likely avenues of enemy approach
- ❑ General unit deployment areas
- ❑ Potential primary and alternate deployment routes.

"Probably the best way to show how to use the plan/order is to relate my first security alert, which came a few weeks later.

"As the battalion operations officer (S3), I received an unclassified message at 1800 hours that an armed element of five to ten persons was planning to attack the depot. The attack was scheduled to occur between 2000 and 0200 hours. In view of previous threats and our vulnerability, the expected attack direction was from the northwest of exclusion area J (see figure Q-1).

"Three units were placed on alert status and told to organize IAW the battalion alert plans and orders. The unit commanders notified were those of the 776th Military Police Company, 30th Ordnance Company, and the 809th MP Detachment (Sentry Dog).

"I called the security alert team (SAT) to place it in a mobile status with the backup alert force (BAF) standing by for deployment. For information only, I also alerted the supporting agency that would provide the augmentation reserve force (ARF).

"Then I established the battalion command post (CP) and prepared the tactical deployment chart (figure Q-1) to brief responding security reserve forces (RF) as they arrived. I pulled copies of the contingency plan/operational order (figure Q-2), which were on file in acetate sleeves.

"At 1812 hours, the 1st Platoon from the 776th MP Company reported for deployment. I took a sleeved op order and entered '1' in the upper right blank and '1st' in the first blank of item 3.b. As I filled in the platoon's assigned objectives, (A, B, C, and D), I noted on my master tactical chart each assigned objective.

"I quickly read the order to the leaders and gave it to the platoon leader. I asked for questions; fielded the few there were; and immediately dispatched the platoon to exclusion area J.

"During the briefing, someone recommended that a fire-team-size element be detached from the reserve force platoon to secure nearby objectives that would be the responsibility of the next reporting platoon. I instructed the platoon leaders to comply with the requirements set forth in the op order.

"Within a few minutes the 1st Platoon leader reported in by radio. The 1st squad and platoon headquarters had secured objective A. The 2d squad was in position at objective B. The 3d squad was set at objective C with one fire team dispatched to secure objective D.

"He also told me that the M60 machineguns were in place with assigned final protective fires (FPF) for interlocking fire.

"When I asked about the early warning dog patrols and listening posts, he said they were in position. Then in code, he gave me their locations. These I noted on my chart with the machinegun placements, which he also gave in code.

"A few minutes later, he contacted me again and asked about the status of his unit command post. I told him I was in the process of briefing the commander.

"I had already entered '2' and '776th MP Co' on another sleeved op order. After the briefing, I gave the order to the commander and the CP element deployed to secure objective E.

"The commander contacted me by radio after a few minutes to tell me that they had made contact with the 1st platoon and its detached squads. All future contact with the command post would be on the command net. I logged '776th' on the chart at objective E for the CP.

"The 2d Platoon arrived, and I briefed the leaders on the situation. I read the op order and gave the platoon leader the sleeved copy with appropriate entries. I told him to standby as a ready strike force to reinforce the 1st Platoon in case of attack. I reminded him that the radio frequency was in the order and that he should make and maintain communication contact with his unit command CP once deployed.

"There are several things about the plan/order concept that make it appealing to commanders and to security managers—it's flexible, it's quick, it's easy, and . . . it works."

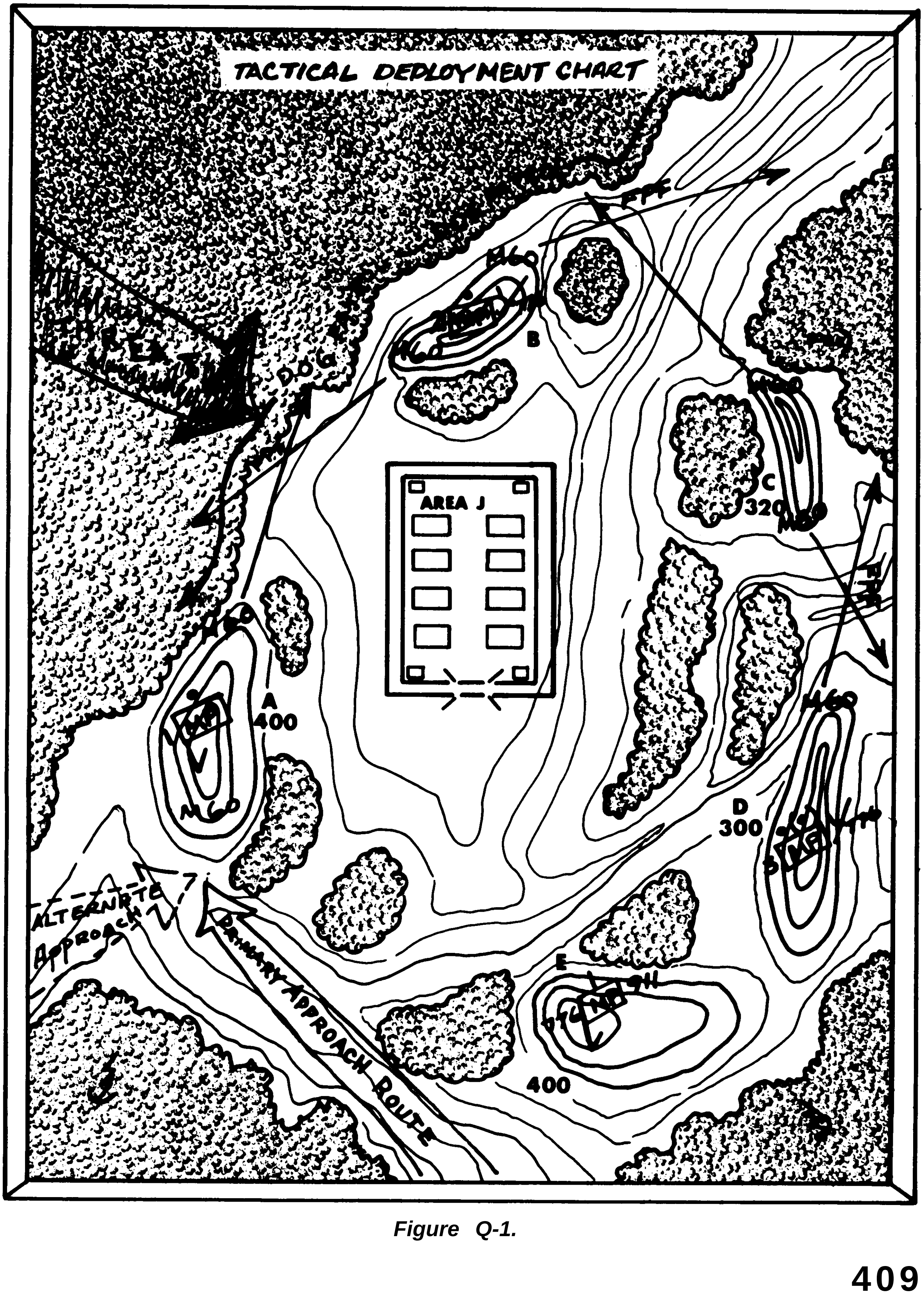

TACTICAL DEPLOYMENT CHART
AREA J
A
400
B
C
320
D
300
E
400
M60
FPF
DOG
ALTERNATE APPROACH
PRIMARY APPROACH ROUTE

Figure Q-1.

Op Order No.______

(CLASSIFICATION)

TASK ORGANIZATION:

1st Platoon, 776th MP Co
2d Platoon, 776th MP Co
3d Platoon, 776th MP Co
1st Sqd, 1st Platoon, 809th MP Det (Sentry/Patrol Dog)

1. SITUATION:

a. Opposing forces. Annex A (Intelligence)
b. Friendly forces. 776th MP Co (TOE 19-97)
c. Attachments and detachments: Task organization

2. MISSION:

Secure predesignated security objectives and key terrain surrounding exclusion Area J.

3. EXECUTION:

a. Concept of operation. 776th MP Co will deploy when alerted to security threat on two routes to secure exclusion Area J (road movement strip map--primary/secondary routes) (Annex B).

b. ______Platoon, 776th MP Co secure and occupy objectives ___________, _____________, ___________, and dispatch a fire team to secure objective _________to dislocate on order back to parent squad and asssist in securing objective _________.

c. 1st Sqd, 1st Platoon, 809th MP Det will deploy well forward of listening posts established by 776th MP Co once the initial objectives and terrain are secured.

d. Coordinating instructions. Coordination with 30th Ord Co and battalion S3 will be accomplished as each assigned security objective is secured. All elements will physically coordinate with squads on adjacent flanks.

4. SERVICE SUPPORT:

No change from the security logistical order.

(CLASSIFICATION)

Figure Q-2 *(first page).*

(CLASSIFICATION)

5. COMMAND AND SIGNAL:

a. Signal. Annex C (Communications/electronics) current CEOI.

b. Command. Company CP will close on objective _______ and coordinate assigned mission.

Acknowledge.

STEVENS
LTC '

OFFICIAL:

/s/Moore
Moore
S3

ANNEXES: A - Intelligence
B - Road Movement Strip Map
C - Communications/Electronics

DISTRIBUTION:

10th Group, S3
30th Ord Co
776th MP Co
809th MP Det
111th Ord Bn, S3

(CLASSIFICATION)

Figure Q-2 continued (last page).

Appendix R

IDS Application and Component Charts

The security manager must be familiar with the various intrusion detection systems to include their characteristics and application. This appendix provides information on principle of activation, application, maintenance supervision problems, nuisance alarms, and credibility rating of each system. Additionally, this appendix outlines a component selection reference.

CHART I. TYPES AND APPLICATION OF INTRUSION DETECTION SYSTEMS

System	Principle of activation	Application	Maintenance supervision problems	Nuisance alarms	Rating
Audio	Sound	Interior only (for vaults and low sound level areas).	Regular inspection to replace inoperative parts.	Frequent (from extraneous sounds).	Not as reliable as ultrasonic.
Sonic	Movement	Interior only	Same as above	Few	More reliable than audio.
Ultrasonic	Movement	Interior only	Same as above	Few	More reliable for protection of rooms.
Microwave	Movement	Interior only	Same as above	Few	Most reliable within patterns set by antennae
Electro-mechanical	Breaking of electric circuit.	Interior only (doors, windows, skylights.	Same as above	Few (metallic foil may break).	Affords minimum protection for buildings and rooms.
Electrostatic (interior)	Movement	Interior only (metal cabinets and safes).	Same as above	Few	Reliable for metal safes and cabinets.
Electrostatic (exterior)	Same as above	Exteriors only (perimeters and also can be attached to side of building).	Same as above. Also to remove snow, ice, and debris from fence.	Many	Best device developed for fence line security.
Closed circuit TV	Visual	Interior and exterior	Same as above. Also to dry lenses.	None	Very effective for remote surveillance.
Photoelectric	Interrupting light beam	Interior and exterior (rooms, halls, gates, an perimeters).	Same as above. Also to clean transmitter and receiver.	Interior (few) exterior (many) (due to fog, rain, birds, etc.).	Interior: reliable when beams are crisscrossed for short distances. Exterior: gates and short distances only.
Vibration	Vibration	Interior only	Same as above	Few	Not as reliable as ultrasonic.

CHART II. COMPONENT SELECTION WORKSHEET

Feature	Material	Recommended sensor	Area coverage per sensor	Notes
*Exterior door	Metal or metal plate	Passive ultrasonic	15 ft by 20 ft	Room sealed from outside sounds.
*Exterior door	Wood or wood substitute	Grid wire kit	160 sq ft per kit.	
*Exterior door	NA	Balanced magnetic switch	One per door—two for dutch or double doors.	
*Interior door	NA	Balanced magnetic switch	One per door—two for dutch or double doors.	
*Interior	Metal or metal plate	Passive ultrasonic	15 ft by 20 ft	Room sealed from outside sounds.
*Interior door	Wood or wood substitute	Grid wire kit	160 sq ft per kit.	

*Exterior door is any door opening into the secure area whether indoors or out; interior door is any door wholly within the secure area.

Feature	Material	Recommended sensor	Area coverage per sensor	Notes
Solid walls, floor, ceiling	Wood plaster	Grid wire kit	160 sq ft per kit.	
Solid walls, floor, ceiling	Metal masonry	Passive ultrasonic	15 ft by 20 ft	Maximum 20 microphones per electronics unit—room sealed from outside sounds.
Open walls, ceiling	Metal wire mesh bars	Grid wire kit	160 sq ft per kit	Additional wall inside required.
Open walls, ceiling	Metal wire mesh bars	Passive ultrasonic	15 ft by 20 ft	Additional wall outside required.
Windows	Glass and open work metal barrier (bars/mesh).	Passive ultrasonic	15 ft by 20 ft	Room sealed from outside sounds.
Windows	Glass and open metal (bars/mesh) barrier (outside).	Capacitance proximity	1200 sq ft of surface area per sensor.	When passive ultrasonic cannot be used.
Windows	Glass and open metal (bars/mesh) barrier (inside).	Vibration	3 ft radius per transducer	When passive ultrasonic cannot be used. Max of 10 transducers per sensor.
Windows	Glass with metal shutter	Passive ultrasonic	15 ft by 20 ft	Room sealed from outside sounds.
Ventilation openings	With metal shutter	Passive ultrasonic	15 ft by 20 ft	Room sealed from outside sounds.
Ventilation openings	With metal shutter	Vibration	3 ft radius per transducer	Max of 10 transducer per sensor
Ventilation openings	NA	Capacitance proximity	1200 sq ft of surface per sensor	For openings larger than 96 sq inches.
Construction openings	Temporary wood covering	Grid wire kit	160 sq ft per kit	When opening can be covered.
Construction openings	NA	Capacitance proximity	1200 sq ft of surface area per sensor.	When opening cannot be covered.
Air conditioner	NA	Capacitance proximity	1200 sq ft of surface area per sensor.	When opening cannot be covered.
Interior motion detection	NA	Ultrasonic motion	20 ft by 30 ft check for shading	Room sealed from outside sounds. Max 20 transceivers per electronics unit.
Weapon removal detection	NA	Magnetic weapon	One wire loop per weapon rack	Detect weapon removal from storage rack.
Storage cabinets	NA	Capacitance proximity	1200 sq ft surface area per sensor.	
Duress	NA	Fixed duress switch	Any number switches	Foot or hand operated switch-alarm signal bypasses local audible alarm.
Duress	NA	Portable duress switch	Any number switches	For roving guard-alarm bypasses local audible alarm.
Control unit	NA	NA	One per secure area.	
Monitor unit	NA	NA	Max—one SI Module per control unit. Enclosures for 1, 5, 25 SI modules.	Provided as visual and audible indication of control unit status.
Local Alarm	NA	NA		Not actuated by duress switches.
Telephone dialer	NA	NA	One per control unit	Used in place of monitor unit.
Type I data transmission system.	NA	NA	One per control unit	Required when rigid wall conduit not used between control unit and monitor unit.

Computer Security

Access— the ability and means to approach, communicate with (input to or receive output from) or otherwise make use of any classified material or any component of an automated data processing (ADP) system.

Access control— operational procedures and physical security measures designed to limit the availability of either classified ADP data in any form, or physical ADP resources, to a recipient.

ADPE— abbreviation for automated data processing equipment.

ADP system damage minimization efforts— efforts and resources whose purpose is keeping to a minimum the ADP dollar loss, adverse impact on ADP, and supported agency operations. Damage minimization efforts can be identified as belonging to system backup, control and warning systems, and drills.

ADP system threat— any danger to ADP installations, hardware, software, communication links, inputs/outputs, or data which could adversely affect ADP system performance, accomplishment of the DPI mission, or ADP system security. They are (human error, sabotage, and theft), accidental, and natural disasters; DPI environmental degradation; and ADP equipment failure threats.

ADP system threat minimization efforts— the sum of hardware and software features, physical and personnel resources, and operating and administrative procedures designed to prevent or minimize the probability of that occurrence. They include physical security measures, personnel training, personnel security procedures, equipment reliability, data security, and communications security (COMSEC).

ADP system security— the hardware/software functions, characteristics, and features; operation procedures, accountability procedures, and both access and entry controls at

the central computer facility, remote computer and terminal facilities; management constraints, physical structures, and devices; and personnel and communications controls needed to provide an acceptable level of protection in a computer system.

Audit— a system for tracing items of data from processing step to processing step, particularly from a machine-produced report or other machine output back to the original source data.

Automatic data processing (ADP)— any phase of data recording, manipulation, remote terminal operations, and other related operations in which data are processed by ADPE; systems inclusive of punched card machines (PCM) and terminal operations.

Backup system— a compatible ADPE configuration at an alternate site which will effectively process mission essential ADP applications in case of damage, environmental disruption, or equipment malfunction.

Breach— successful defeat of security controls that could result in penetration of the system. Examples include, but are not limited to, operation of user code in control program mode, unauthorized acquisition of ID password or file access passwords, and not using prescribed operating system mechanisms to gain a file.

Data— information or symbology contained in storage, registers, buffers, documents, cards, tapes, drums, and communications links.

Data processing (DP) installation/ activity (DPI/A)— any facility, room, or building housing ADPE, storing tapes, cards, or other media used to perform the ADP support mission. It does not include the housing of auxiliary power sources, or output processing areas (unless they are collocated with the DPI/A). A DPA, by nature of its mission and resources, can function independently within the DPI. It normally has a separate manager and a separate ADPE configuration.

Data security— protection of data from either accidental or unauthorized modification, destruction, or disclosure; sabotage; malicious; mischief; theft; or mutilation.

Debug/test program procedures— methods used to locate and correct any errors in a computer program.

Disaster— an occurrence that could completely prevent a DPI from accomplishing its normally assigned mission. (This includes fire, major water damage, extended power failure, sabotage, etc.).

DP equipment malfunction— temporary failure of any equipment to function as designed when required.

Drills— simulations designed to test the performance of resources, systems, procedures, and personnel against standards established for threat minimization.

Edit controls— measures designed to identify rearrangement of data or information. The editing may involve deletion of unwanted data, selection of pertinent data, and the testing of data for reasonableness and proper range.

Entry— the ability and means to approach, communicate with (input to or receive output from), or otherwise make use of either unclassified material or any component of an automated data processing system.

Entry controls— operational procedures and physical security measures designed to limit availability of either unclassified ADP data in any form, or physical ADP resources, to a recipient.

Environmental disruption— improper concentrations of rust, dust, humidity, smoke, temperature, foreign matter, etc., in a room housing ADPE.

Erase/degauss procedure— a protective measure that involves overwriting or rerecording on a magnetic surface so as to

completely erase the original data.

ESI— abbreviation for especially sensitive information.

Human error— unintentional act of a human that results in the occurrence or probable occurrence of a disaster, environmental disruption, or equipment malfunction; or the unintentional addition, deletion, or substitution of data in any file, record, or program.

Inputs/outputs (I/O)— physical media processing information used as an input or output in an ADP system. (Includes documents, punch cards, magnetic tape, punched tape, machine printouts, and similar media. Excludes the data or information displayed or the information on the media.)

MISM— abbreviation for management information system material.

Multilevel security mode— a mode of operation under an operating system (supervisor or executive program) which provides a capability permitting various levels and categories or compartments of material to be concurrently stored and processed in an ADP system. In a remotely accessed resource-sharing system, the material can be selectively accessed and manipulated from variously controlled terminals by personnel having different security clearances and access approvals. This mode of operation can accommodate the concurrent processing and storage of two or more levels of classified data, or one or more levels of classified data with unclassified data depending upon the constraints placed on the systems.

Operating system— an integrated collection of service routines for supervising the sequencing and processing of programs by a computer.

Passwords— a word or string of characters, uniquely associated with a use, which either authenticates a user or identifies a defined system resource, such as a program.

Penetration— a successful unauthorized entry and/or access into a system.

Physical security measures— protective actions against threats to the central computer facility, its remote computer and terminal facilities, the related tape/disk libraries, and the supporting areas achieved by locks, guards, badges, personnel security clearances and administrative control measures outside the computer as well as measures required for the protection of the structures housing the computer. Associated with these measures should be provisions for off-site storage of data and for backup systems.

Remote terminals— remotely located devices used to input data to and receive output data from a central computer system by communication lines or cables. Generally, these devices are physically located in an area separated from the central site.

Remotely accessed/entered resource sharing computer system— a computer system that includes one or more central processing units, peripheral devices, remote terminals, and communications equipment or interconnection links, which allocates its resources to one or more users, and which can be used from terminals located outside the central computer facility.

Resource sharing computer facility— a computer facility that uses its resources, including I/O devices, storage, central processor (arithmetic and logic units), control units, and software processing capabilities to enable two or more users to manipulate data ‘and process coresident programs in an apparently simultaneous manner. The term includes systems with one or more of the capabilities commonly referred to as time-sharing, multiprograming, multiaccessing, multiprocessing, or concurrent processing.

Routine, utility— a standard routine used to assist in the operation of the computer, such as a conversion routine, a sort routine, or a printout routine.

Sensitive information— unclassified data which a commander designates for special handling, including individuals authorized to receive it.

SIOP— abbreviation for single integrated operational plan.

Software lockout— prohibition of access to information through programing techniques rather than hardware lockout or physical means.

System backup— a computer or peripheral equipment normally specifically designated and available to provide computer processing/services if the primary computer system or its peripherals are destroyed or otherwise unavailable. Backup equipment may be collocated with the primary system or at another installation.

Tempest— refer to AR 530-4.

Warning system— any device or procedure designed to alert personnel to a specified event or threat.

Intrusion Detection Systems (IDS)

Actuator— in commercial security systems, a holdup button, magnetic switch or thermostat that will cause the system to alarm.

Annunciator (monitor)— a visual or audible signaling device that indicates conditions of associated circuits. Usually, this is accomplished by activation of a signal lamp and audible sound.

Antenna— a conductor or system of conductors for radiating or receiving electromagnetic waves.

Balanced magnetic switch— a magnetically operated switch designed to detect the opening of a secured door, window, or other closure. In addition, it detects attempts to defeat the switch by substituting a magnetic field and may have provisions for internal adjustments and detection of switch tampering attempts.

Capacitance— the property of two or more objects which enables them to store electrical energy in an electrostatic field between them.

Capacitance proximity sensor— records a change in capacitance or electrostatic fields to detect penetration through windows, ventilators, and other openings, and can be used to detect attempted penetration into safes or storage cabinets.

Conductor— material which transmits electric current. Wire and cable are conductors. Also called signal transmission lines.

Contacts— parts of a switch or relay which by touching or being separated permit electric current to flow or cease to flow. Frequently and improperly used to designate an entire magnetic switch or balanced magnetic switch component.

Control unit— the terminal box for all sensors. It receives alarm and tamper signals and transmits these signals to the local audible alarm and/or monitor unit. It provides the primary and backup power for all sensors; activates and deactivates the system.

Data transmission system— Component consisting of a data transmitter in the control unit and a data receiver in the monitor unit and is the communication link used to pass alarm and equipment status signals from the control unit to the monitor unit over a wire transmission line or by radio frequency.

Doppler— the effect of compression of expanding sound or radio frequencies reflected from or originating from a moving object.

Fail-safe— a term applied to a system designed so that if a component fails to function properly, the system, will, by a

signal or otherwise, indicate its incapacity.

False alarm— activation of sensor(s) for which no cause can be determined.

Fixed duress sensor— an emergency notification device, switch, or button manually operated by personnel needing assistance.

Grid wire sensor— detects forced entry through walls, floors, ceilings, doors, and other barriers by the break-wire method.

Intrusion detection system— the combination of components, including sensors, control units, transmission lines, and monitor units integrated to operate in a specified manner.

Intrusion detection sensors— devices that initiate alarm signals by sensing the stimulus, change, or condition for which they were designed.

Joint-Service Interior Intrusion Detection System (J-SIIDS)— developed as a standard detection system for joint-service application for protection of military arms rooms and other inside areas.

Local audible alarm— an electronic screamer or bell for outdoor or indoor use in the vicinity of the protected area.

Magnetic contact/simple magnetic switch— consists of two separate items, a magnetically actuated switch and a magnet. The switch is usually mounted in a fixed position (door frame or safe) opposing the magnet, which is fastened to a hinged or sliding door. When the movable barrier is opened, the magnet moves with it and the switch opens. Magnetic contacts are usually connected so that the switch is closed while the magnet is near. This allows the electric current to flow. When the door or window is open, the magnetic contact opens. This stops the electric current flow, causing an alarm.

Magnetic weapon sensor— a wire loop assembly used to detect the magnetic field disturbance caused by the removal of a weapon from a weapons rack.

Microwave sensor— a radio/radar frequency (RF) transceiver having a frequency range of GHz (billion cycles per second) which detects motion through the Doppler shift effect.

Monitor— a device that senses and reports on the condition of a system, commonly used interchangeably with the terms, monitor unit, monitor panel(s), status indicator module, annunciator, and other similar terms.

Motion sensor— detects movement inside the area to be protected.

Nuisance alarm— the result of a sensor activation caused by accident, neglect, malfunction, or natural causes, such as wind, lightning, or thunder. Often improperly called false alarm.

Overload— a condition in which an electrical device draws a current greater than its rated capacity.

Passive ultrasonic sensor— detects the sounds of forced entry through walls, ceilings, and doors.

Penetration sensor— detects entry through doors, windows, walls, or any other openings into the protected area.

Photoelectric system— usually supplied as two separate units, a transmitter and receiver. A light beam is transmitted to the receiver. Any interruption of this light causes an alarm.

Point sensor— detects removal or attempted removal of an object from its storage container.

Radio— radio frequency (RF) transceiver having a frequency range of 100 MHz (million cycles per second) to 1 GHz (billion cycles per second).

Sonic— having a frequency within the hearing distance of the human ear.

Supervised line— a conductor which (if cut, broken, shorted, or otherwise tampered with) will cause a change in status indicated at a monitoring unit.

Telephone dialer— a device, normally installed within the protected area, that automatically dials preselected telephone numbers upon sensor activation and provides a prerecorded message notifying of intrusion.

Ultrasonic— the frequency range of sound that is above the capabilities of normal human hearing. In intrusion detection systems it usually varies between 21,500 and 26,000 Hz (cycles per second).

Ultrasonic motion sensor— detects by frequency shift (doppler) the motion of an intruder inside the protected area.

Vibration sensor— detects forced entry through metal barriers placed over windows and ventilators or attempts to drill, saw, or cut through walls, ceilings, floors, or doors.

Nuclear Reactors

Access-close physical proximity to special nuclear material, control consoles, or the reactor, which provides the opportunity for tampering with or damaging the material, consoles, or reactor. Posts must be established to control access.

Exception— permanent exclusion from specific requirements based on case-by-case determination that unique circumstances at a given unit, facility, or installation are such that conformance to established standards and measures is impossible, highly impractical, exceptionally costly, unnecessary due to measures exceeding those prescribed, or not in the best interest of the US Government.

Nuclear reactor— a facility in which fissionable material is used in a self-supporting chain reaction (nuclear fission) to produce heat and/or radiation for both practical application and research and development (AR 310-25). A nuclear reactor system includes reactors and their associated components, auxiliary systems, and engineered safeguards.

Nuclear reactor facility— a nuclear reactor system, the associated buildings, auxiliary equipment, and reactor staff required for its operation, maintenance, and support. The term includes both power and research nuclear reactor facilities.

Reactor commander— chief of the organizational unit directly responsible for operation of a nuclear reactor facility, including the reactor staff.

Response force— personnel, other than those performing security functions at the facility, whose mission is to augment the security force as required.

Responsible commander— the organizational element commander or director to whom the reactor commander reports.

Restricted or vital area— any area, designated by the reactor facility commander, to which access is restricted or controlled for reasons of security or to safeguard property or material.

Limited area— a restricted area that surrounds one or more exclusion or vital areas.

Exclusion/vital area— a restricted area which contains special nuclear material, a nuclear reactor, or control consoles.

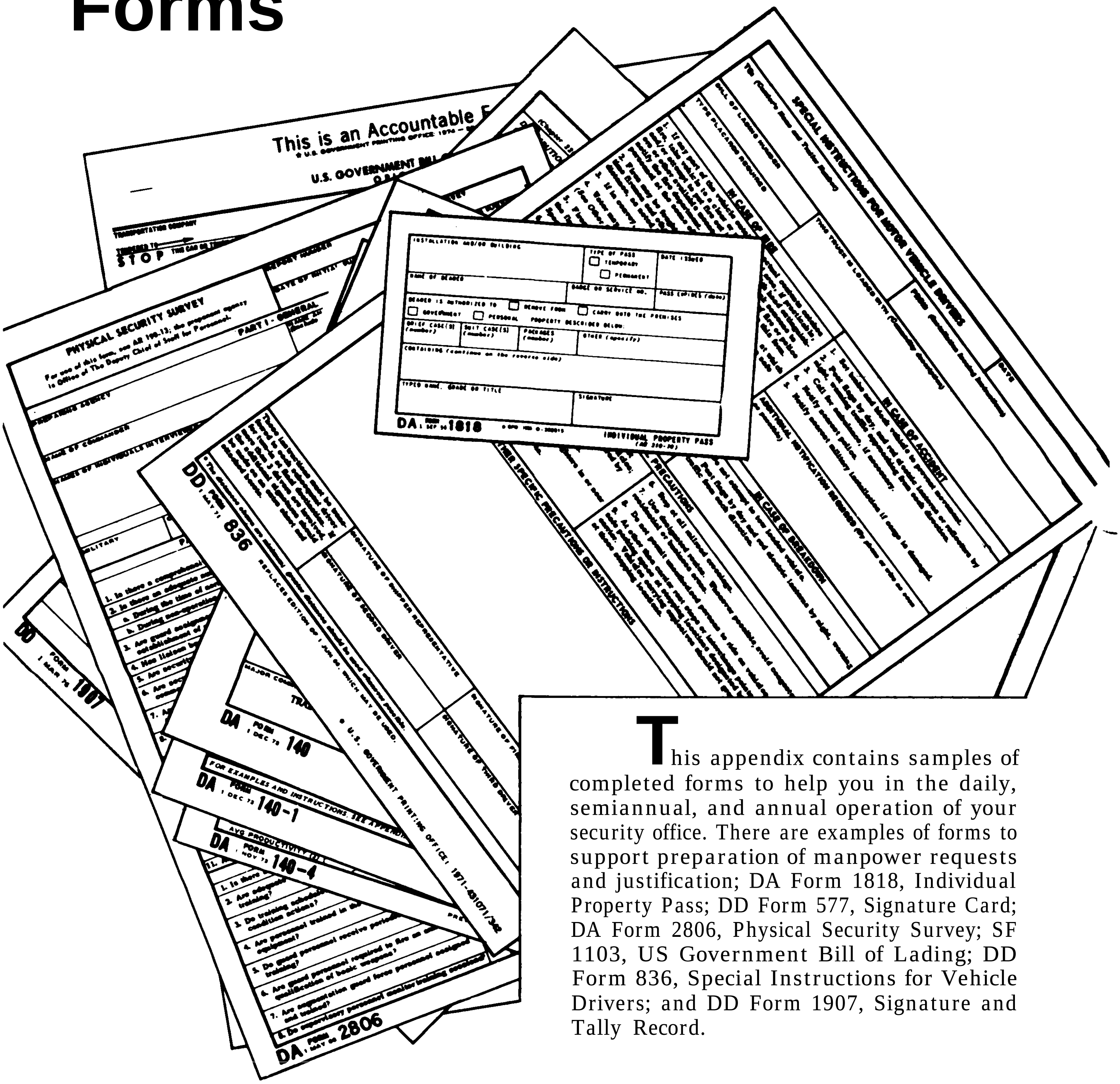
Security force— personnel performing security duties at the nuclear reactor facility.

Special nuclear material (SNM)— plutonium, uranium enriched in the isotope 233 or in the isotope 235; any other material which the US Nuclear Regulatory Commission determines to be special nuclear material; or any material artificially enriched by any of the foregoing. SNM does not include source material.

Waiver— a temporary exemption, for not more than 1 year, from a specified requirement. (Requests for waivers or exceptions referred previously will include circumstances requiring the action and compensatory measures taken to achieve a comparable degree of security. Requests will be forwarded through command channels to HQDA.)

Appendix T

Forms



This appendix contains samples of completed forms to help you in the daily, semiannual, and annual operation of your security office. There are examples of forms to support preparation of manpower requests and justification; DA Form 1818, Individual Property Pass; DD Form 577, Signature Card; DA Form 2806, Physical Security Survey; SF 1103, US Government Bill of Lading; DD Form 836, Special Instructions for Vehicle Drivers; and DD Form 1907, Signature and Tally Record.

DD Form 577, Signature Card, is best used in the physical security environment in support of DA Form 1818. Each activity or installation commander should require that signature cards be prepared on persons authorized to allow property to be removed from the activity or installation.

Each card should be prepared in triplicate. The first is for the person authorizing release of the property. A second copy is filed at the local security office. The third copy goes to the security guard at the gate or control point, for immediate reference.

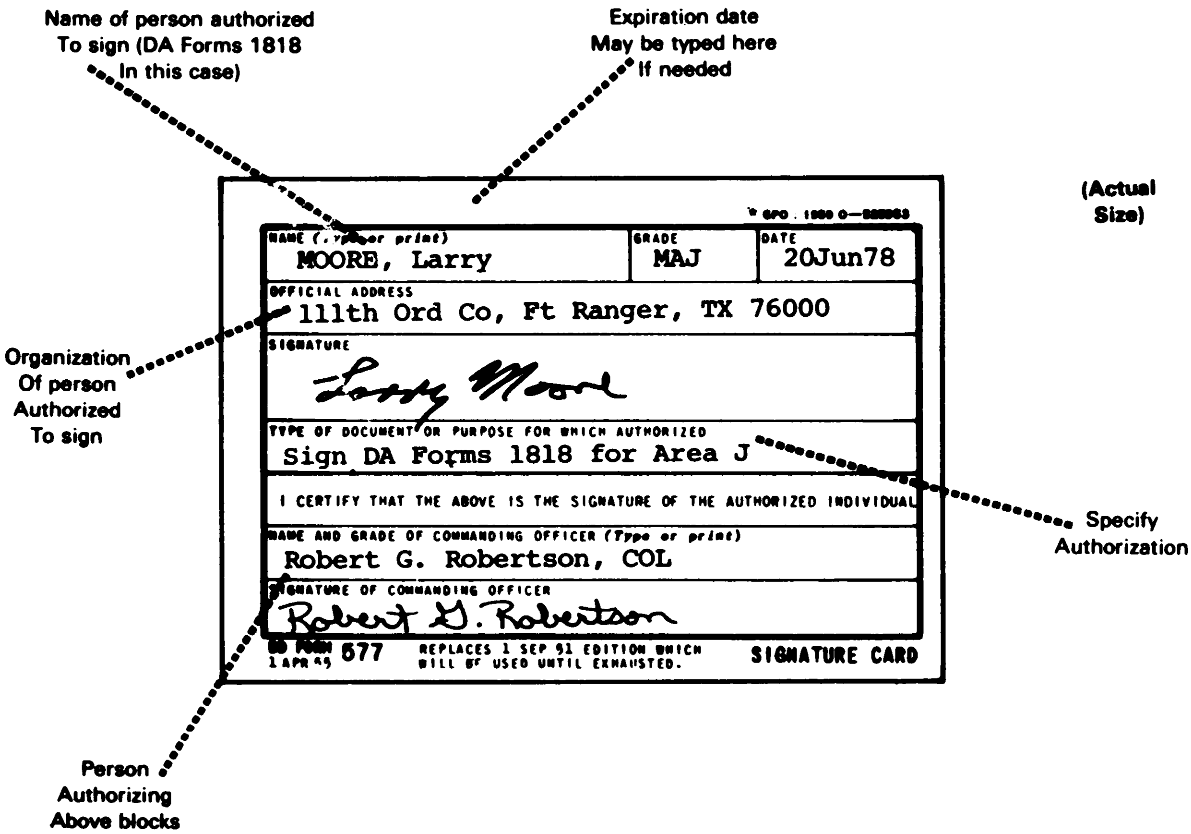


Figure T-1—Sample signature card.

Sample DA Form 1818

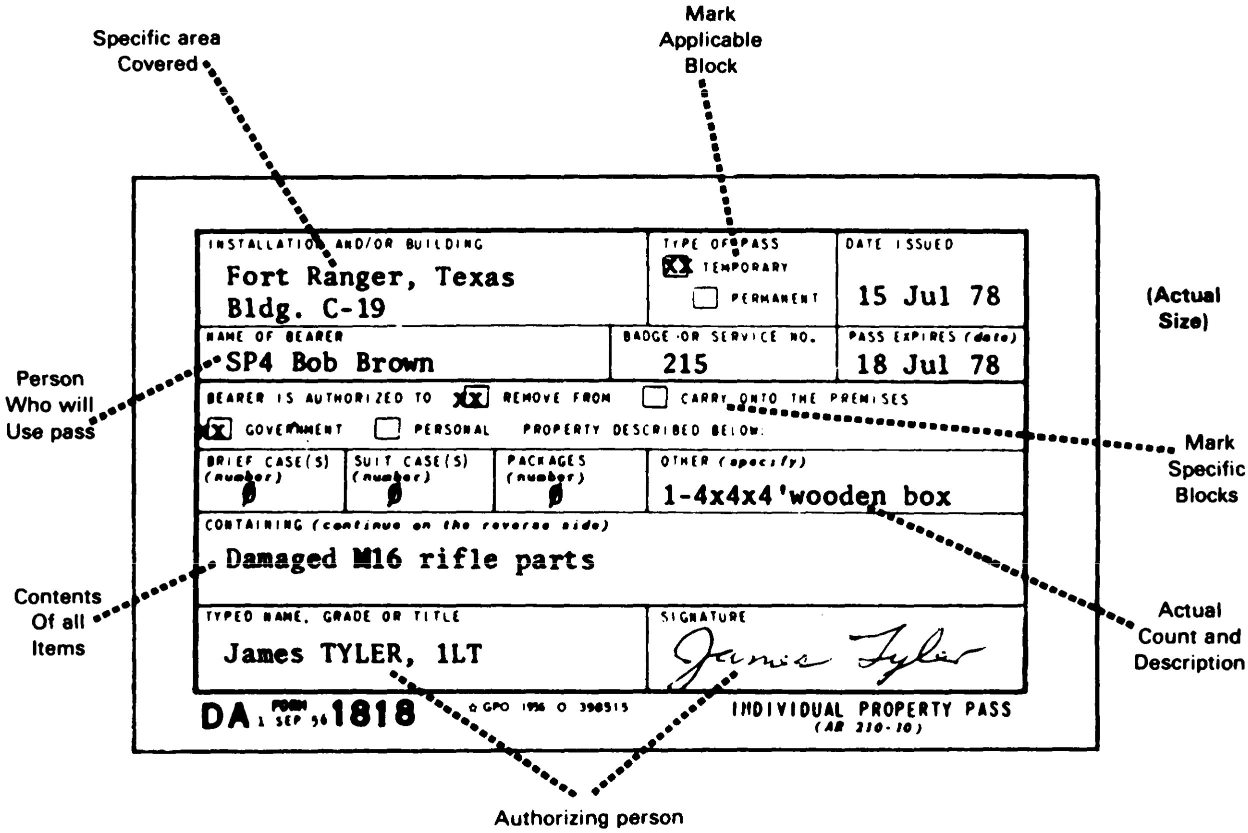


Figure T-2—Sample individual property pass.

One essential element of an installation's overall physical security program is DA Form 1818, individual Property Pass. It acts as a check and balance for authorized removal of property from an activity or installation.

A property pass may be temporary or permanent with a valid use of 24 hours to 90 days, depending on local policy. For best accountability and control of the forms and inspection of installation property, you should control the forms from one location, preferably the physical security office.

SPECIAL INSTRUCTIONS FOR MOTOR VEHICLE DRIVERS

DATE: 31 Oct 79

TO: *(Carrier's Name and Trailer Number)* Deans Transportation Co, Trlr No: 173

FROM: *(Installation Issuing Instructions)* Transportation Officer, Ft McClellan, AL 36205

BILL OF LADING NUMBER: M-1234567

TYPE PLACARDS REQUIRED: Class A

THIS TRUCK IS LOADED WITH *(Commodity description)*: Explosives, rockets, ammunition with explosive projectile, rockets, HE, 66MM AT (Unserviceable) Class A

IN CASE OF FIRE

1. If any part of the vehicle outside of actual contents catches fire, take vehicle to a clear or uninhabited area, if practicable, and/or attempt to put fire out immediately with hand extinguishers or other available means. If practicable, ask someone to notify the fire department. Call to the attention of fire or police personnel at the scene of the fire the information on this form.
2. Fires may be fought until the flames reach the cargo, at which time firemen and other personnel should be withdrawn to a safe distance, as noted in 5 and 6 below.
3. If in convoy, other trucks proceed to safe distance.
4. Water may be used on this cargo ☐ Yes ☐ No *(See Other Specific Precautions or Instructions below)*
5. Firemen should not approach closer than 1200 feet* from the fire when the fire has reached the cargo. *(See Other Specific Precautions or Instructions below)*
6. Public should not approach closer than 2000 feet* from fire.
7. As soon as practical, notify the nearest military installation.

IN CASE OF ACCIDENT

1. Set brake and block vehicle to prevent movement.
2. Post flags by day, and red electric lanterns or reflectors by night, warning traffic approaching from each direction.
3. Call for ambulance, if necessary.
4. Notify nearest police.
5. Notify nearest military installation if cargo is damaged.

ADDITIONAL NOTIFICATION REQUIRED *(By phone or wire as soon as possible)*

T.O. FtMcClellan,AL AC 205 238-3433/3321
T.O. Big Job Army Ammunition Plant, New Harmony, IN AC 214 838-2515

IN CASE OF BREAKDOWN

1. Do not attempt to tow loaded vehicle.
2. Post flags by day and red electric lanterns by night, warning traffic from each direction.

GENERAL PRECAUTIONS

1. While operating over public roads, keep at least 300 feet from trucks loaded with explosives or other dangerous articles; a greater minimum distance must be maintained if required by state or municipal regulations.
2. Protect the public from the hazards of the cargo.
3. Do not allow smoking or use of matches or lighters in or near the vehicle.
4. Obey all state and local traffic regulations.
5. Do not exceed posted speed limits.
6. Stop at all railroad crossings.
7. Use designated routes. Whenever possible, avoid congested residential or business areas.
8. Do not permit unauthorized persons to ride on vehicles.
9. At other than carrier rest stops or interchange points, select safe parking space at stopping locations designated by the carrier. Vehicles carrying explosives should not group together at these stopping locations.

OTHER SPECIFIC PRECAUTIONS OR INSTRUCTIONS

PRINCIPALLY A MISSILE (FRAGMENT) HAZARD. MAINTAIN THE MINIMUM DISTANCES AS LISTED ABOVE: SPECIAL PRECAUTIONS -- "PREPARE TO FIGHT INCIPIENT FIRES STARTED BY THE EXPLOSION."

These instructions must be transferred to each subsequent driver for turn-in at final destination. If more than 3 drivers are involved, the additional signatures should be made on an extra sheet and attached hereto.

SIGNATURE OF SHIPPER REPRESENTATIVE: LAWRENCE MOORE, MAJ, TC, TO:TA FOR TO

SIGNATURE OF FIRST DRIVER

SIGNATURE OF SECOND DRIVER

SIGNATURE OF THIRD DRIVER

* *The distances shown are minimum; greater distances should be used whenever possible.*

DD FORM 1 MAY 71 836 REPLACES EDITION OF 1 JUN 66, WHICH MAY BE USED.

★ U.S. GOVERNMENT PRINTING OFFICE: 1971-431071/342

Figure T-3—Sample driver instruction sheet.

To help insure that items are delivered as safely as possible, special instructions for motor vehicle drivers is essential. This is accomplished through use of DD Form 836, Special Instructions for Motor Vehicle Drivers.

The form prescribes actions required of vehicle drivers in case of fire or accident. These include notification requirements, precautions, and actions to initiate during breakdown. All drivers should be briefed on requirements involving motor vehicle shipments and given a completed DD Form 836. The form must be kept in each driver's possession. It is essential that this form be linked to the shipment through use of the bill of lading number.

SIGNATURE AND TALLY RECORD

(Chapter 226, AR 55–355/NAVSUPINST 4600.70/AFM 75–2/MCO P4600.14A/DSAR 4500.3)

FORM APPROVED
OMB No. 49–R0410

DISTRIBUTION INSTRUCTIONS: (1) The SHIPPER will prepare Copy 1 thru 5 and retain Copy 5. Deliver Copy 1 thru 4 to the "origin carrier".
(2) The CARRIER will deliver Copy 1 thru 4 to the "destination carrier".
(3) The DESTINATION CARRIER will attach Copy 1 (reflecting all signatures) and SF Form 1113 (Public Voucher For Transportation Charges) to the original Government Bill of Lading and forward for payment. Copy 2 and 3 will be delivered to the "consignee". Retain Copy 4.
(4) The CONSIGNEE will mail Copy 2 to the shipper and retain Copy 3.

SECTION A – To be completed by the SHIPPER.

1. NAME OF SHIPPER & ORIGIN Transportation Officer Ft McClellan, AL 36205	2. PROTECTIVE SERVICE REQUESTED (D) Dual Driver Protective Service	
	3. GBL OR CBL NUMBER M-1234567	
4. NAME OF CONSIGNEE & DESTINATION T.O. Big Job Army Ammunition Plant New Harmony, IN 71234	5. PERMIT NUMBER *(if any)*	
	6. TRANSPORTATION CONTROL NUMBER W31VH6-6355-9401	
7. ROUTING Deans Transportation Company	8. WEIGHT 11,244	9. CUBE 705.5
10. SPECIAL INSTRUCTIONS	11. DATE SHIPMENT TENDERED TO CARRIER & NAME OF CARRIER 31 Oct 79	
12. NUMBER OF PIECES & TYPE OF PACKAGE(S) *(for unsealed loads only)* OR CONVEYANCE IDENTIFICATION & SEAL NUMBERS *(for sealed loads only)* 83 Bx	13. FREIGHT CLASSIFICATION DESCRIPTION Class A Exp, rockets, ammo with exp proj, rockets, HE, 66MM	

SECTION B – To be completed by each person accepting custody of classified or protected material requiring the use of transportation protective service during transit.

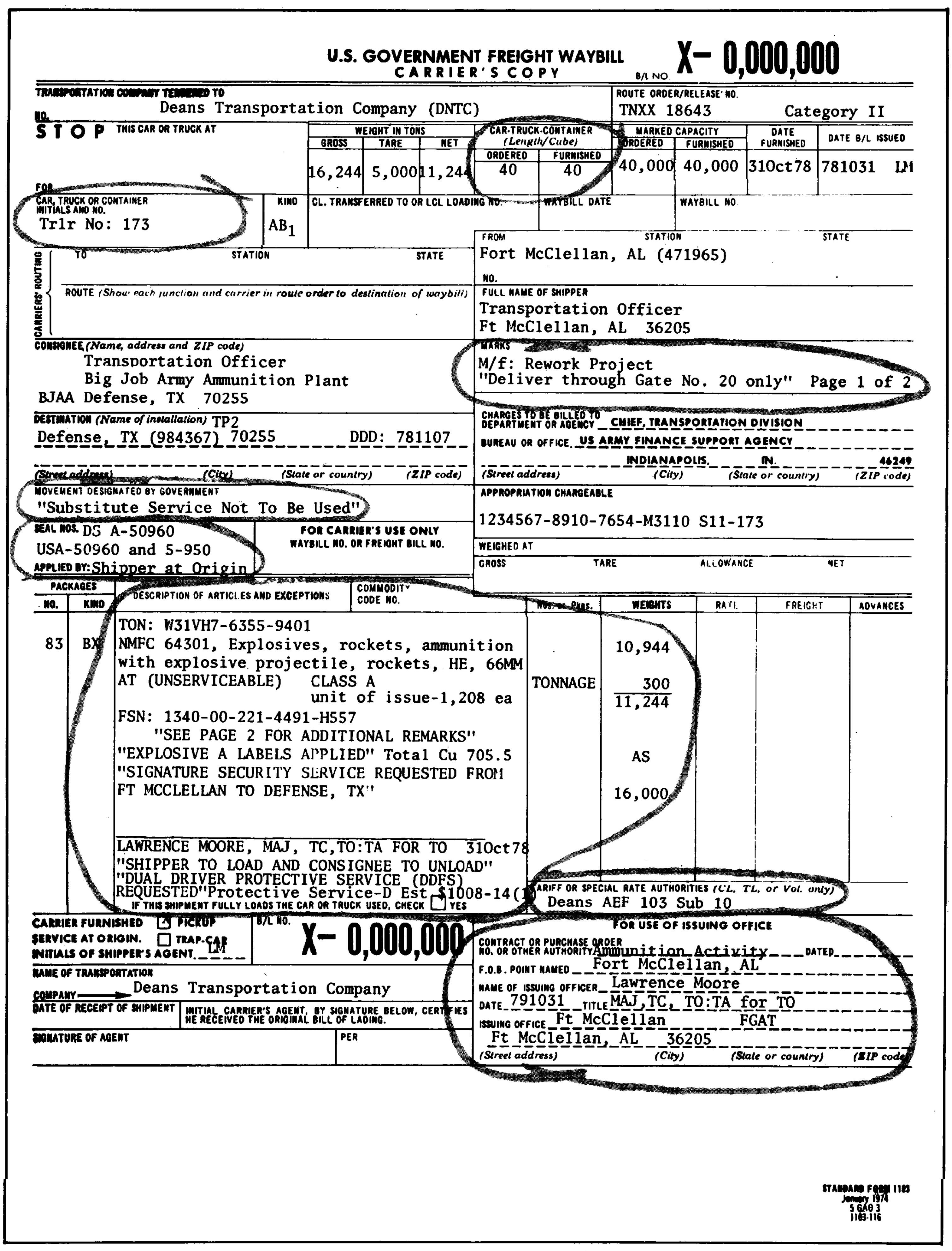
14. PRINT NAME OF PERSON AND COMPANY REPRESENTED	STATION INTERCHANGE POINT DESTINATION	SIGNATURE OF PERSON ACCEPTING CUSTODY	TIME/DATE
J.D. Howard	Anniston	J. D. Howard	3 Nov 79

DD FORM 1 MAR 76 1907 REPLACES EDITION OF 1 MAR 73 WHICH WILL BE USED UNTIL EXHAUSTED.
Destination Carrier – COPY 4

Figure T-4—Signature and tally record sample.

DD Form 1907, Signature and Tally Record, must be completed by the shipper and agency or person accepting custody of classified or protected material. The record must be initiated when transportation protective service is used during transit.

Each Signature and Tally Record must be linked to its corresponding bill of lading through use of the transportation control number. AR 55-355 establishes policy for the form.



U.S. GOVERNMENT FREIGHT WAYBILL
CARRIER'S COPY
B/L NO. X- 0,000,000

TRANSPORTATION COMPANY TENDERED TO: Deans Transportation Company (DNTC)
ROUTE ORDER/RELEASE NO.: TNXX 18643 Category II

STOP THIS CAR OR TRUCK AT

WEIGHT IN TONS GROSS	TARE	NET	CAR-TRUCK-CONTAINER (Length/Cube) ORDERED	FURNISHED	MARKED CAPACITY ORDERED	FURNISHED	DATE FURNISHED	DATE B/L ISSUED
16,244	5,000	11,244	40	40	40,000	40,000	31Oct78	781031 LM

FOR CAR, TRUCK OR CONTAINER INITIALS AND NO.: Trlr No: 173
KIND: AB1
CL. TRANSFERRED TO OR LCL LOADING NO.
WAYBILL DATE
WAYBILL NO.

CARRIERS' ROUTING: TO STATION STATE
ROUTE (Show each junction and carrier in route order to destination of waybill)

FROM STATION STATE: Fort McClellan, AL (471965)
NO.
FULL NAME OF SHIPPER: Transportation Officer Ft McClellan, AL 36205

CONSIGNEE (Name, address and ZIP code): Transportation Officer Big Job Army Ammunition Plant BJAA Defense, TX 70255

MARKS: M/f: Rework Project "Deliver through Gate No. 20 only" Page 1 of 2

DESTINATION (Name of installation) TP2 Defense, TX (984367) 70255 DDD: 781107
(Street address) (City) (State or country) (ZIP code)

CHARGES TO BE BILLED TO DEPARTMENT OR AGENCY: CHIEF, TRANSPORTATION DIVISION
BUREAU OR OFFICE: US ARMY FINANCE SUPPORT AGENCY
INDIANAPOLIS, IN. 46249
(Street address) (City) (State or country) (ZIP code)

MOVEMENT DESIGNATED BY GOVERNMENT: "Substitute Service Not To Be Used"

APPROPRIATION CHARGEABLE: 1234567-8910-7654-M3110 S11-173

SEAL NOS. DS A-50960 USA-50960 and 5-950
APPLIED BY: Shipper at Origin
FOR CARRIER'S USE ONLY WAYBILL NO. OR FREIGHT BILL NO.

WEIGHED AT
GROSS TARE ALLOWANCE NET

PACKAGES NO. KIND | DESCRIPTION OF ARTICLES AND EXCEPTIONS | COMMODITY CODE NO. | NO. OF PKGS. | WEIGHTS | RATE | FREIGHT | ADVANCES

83 BX
TON: W31VH7-6355-9401
NMFC 64301, Explosives, rockets, ammunition with explosive projectile, rockets, HE, 66MM AT (UNSERVICEABLE) CLASS A
unit of issue-1,208 ea
FSN: 1340-00-221-4491-H557
"SEE PAGE 2 FOR ADDITIONAL REMARKS"
"EXPLOSIVE A LABELS APPLIED" Total Cu 705.5
"SIGNATURE SECURITY SERVICE REQUESTED FROM FT MCCLELLAN TO DEFENSE, TX"

TONNAGE 10,944 300 11,244 AS 16,000

LAWRENCE MOORE, MAJ, TC,TO:TA FOR TO 31Oct78
"SHIPPER TO LOAD AND CONSIGNEE TO UNLOAD"
"DUAL DRIVER PROTECTIVE SERVICE (DDPS) REQUESTED" Protective Service-D Est $1008-14(
IF THIS SHIPMENT FULLY LOADS THE CAR OR TRUCK USED, CHECK ☐ YES

TARIFF OR SPECIAL RATE AUTHORITIES (CL, TL, or Vol. only): Deans AEF 103 Sub 10

CARRIER FURNISHED SERVICE AT ORIGIN. ☒ PICKUP ☐ TRAP-CAR
INITIALS OF SHIPPER'S AGENT: LM
B/L NO. X- 0,000,000
NAME OF TRANSPORTATION COMPANY: Deans Transportation Company
DATE OF RECEIPT OF SHIPMENT | INITIAL CARRIER'S AGENT, BY SIGNATURE BELOW, CERTIFIES HE RECEIVED THE ORIGINAL BILL OF LADING.
SIGNATURE OF AGENT | PER

FOR USE OF ISSUING OFFICE
CONTRACT OR PURCHASE ORDER NO. OR OTHER AUTHORITY: Ammunition Activity DATED
F.O.B. POINT NAMED: Fort McClellan, AL
NAME OF ISSUING OFFICER: Lawrence Moore
DATE: 791031 TITLE: MAJ, TC, TO:TA for TO
ISSUING OFFICE: Ft McClellan FGAT
Ft McClellan, AL 36205
(Street address) (City) (State or country) (ZIP code)

STANDARD FORM 1103 January 1974 5 GAO 3 1103-116

Figure T-5—GBL sample with critical areas circled.

Standard Form 1103, US Government Bill of Lading, is an extremely critical document in accountability of goods and property shipped by Government and commercial agencies.

The document may be manipulated to cover theft of items. Security force members must know how to review and check a bill of lading to detect such tampering. Critical areas for members to be aware of are circled on the sample form that follows.

One idea to speed effectiveness of new personnel and to insure complete review of each document by gate personnel has been proven in the field. This security manager had a large (6-feet by 8-feet) wooden poster painted to hang on the gate house outer wall. The poster could be read by guards as they checked trucks into the facility. It had all critical areas circled in red. No losses were experienced through bill of lading manipulation after implementation of this aid. (His circled areas correspond to those on the sample SF 1103 that follows. You may not need all of these or you may need to add others.)

153-846 0 - 94 - 18 (Fold-in No. 4)

PHYSICAL SECURITY ~~SURVEY~~ INSPECTION
For use of this form, see AR 190-13; the proponent agency is Office of The Deputy Chief of Staff for Personnel.

REPORT NUMBER	DATE OF SURVEY
15-76	5-7 Feb 76
DATE OF INITIAL SURVEY	DATE OF PREVIOUS SURVEY

ANNUAL - UNANNOUNCED

PART I - GENERAL

PREPARING AGENCY: Office of the Provost Marshal, Ft Custer, OK 39999	NAME AND LOCATION OF INSTALLATION OR FACILITY SURVEYED (Include ZIP Code): Ammunition Storage Point, Big Horn Rd, Ft Custer, OK 39999
NAME OF COMMANDER: Peter Reno, MAJ	NAME OF SECURITY OFFICER: Alan Colt, 1LT
NAMES OF INDIVIDUALS INTERVIEWED: Peter Reno, MAJ, Officer in Charge; Alan R. Colt, 1LT, Security Officer; Red R. Buckle, MSG, NCOIC; (See attached sheets)	NAMES OF SURVEY PERSONNEL (Grade, Title and organization): Horace S. Bull, SFC, Physical Security Inspector, Office of the Provost Marshal; (See attached sheets)

STRENGTHS: MILITARY	CIVILIAN	SECURITY FORCE	INSTALLATION ACREAGE	NUMBER OF BUILDINGS
5	4	7	24	14

PART II - GUARDS

	YES	NO
1. Is there a comprehensive physical security plan?	X	
2. Is there an adequate number of guards assigned -	X	
a. During the time of normal operation?	X	
b. During non-operational hours?	X	
3. Are guard assignments rotated to prevent establishment of routines?	X	
4. Has liaison been established with civil authorities?	X	
5. Are security supervisory personnel school trained?	X	
6. Are security personnel delegated authority commensurate to their duties?	X	
7. Are adequate records maintained on reported and/or investigated incidents?	X	
8. Are all security personnel equipped with all authorized equipment?	X	
a. Are security forces armed?	X	
b. Has authority for use of weapons been included in guard orders?	X	
c. Are security forces knowledgeable on the use of weapons and understand the limits of their jurisdiction?	X	
9. Could sentry dog teams be properly utilized?	REMARK	
10. Are security personnel required to meet reasonable physical, mental and loyalty standards?	X	
11. Are guard orders posted, current and understood?	X	

PART III - TRAINING

	YES	NO
1. Is there a current training program in effect?	X	
2. Are adequate records maintained on individual training?	X	
3. Do training schedules include emergency condition actions?	X	
4. Are personnel trained in the use of emergency equipment?	X	
5. Do guard personnel receive periodic refresher training?	X	
6. Are guard personnel required to fire an annual qualification of basic weapons?	X	
7. Are augmentation guard force personnel assigned and trained?	X	
8. Do supervisory personnel monitor training sessions?	X	

PART IV - PREVENTION OF UNAUTHORIZED ENTRY

	YES	NO
1. Is there an adequate perimeter barrier?	X	
2. Is perimeter barrier properly posted?	REMARK	
3. Are all openings in the perimeter barrier guarded or secured?	X	
4. Is protective lighting used?	X	
5. If there is no protective lighting is it needed?	NA	
6. Is vehicle search authority established?	X	
7. Is there a positive system for the identification of employees?	X	
8. Is there a positive package control system in effect?	X	
9. Are visitors and non-employees escorted?	X	
10. Is a visitor register maintained?	X	
11. Does the system establish procedures for identifying, admitting and control of visitors, contract personnel, vendors, etc.?	X	
12. Is there an effective system for the control of vehicles, railroad cars and other convey access and their contents into, or out of the installation area?	X	
13. Is there an installation traffic control plan?	NA	
14. Has a satisfactory parking control system been established?	X	
15. Is vehicle registration required?	NA	

PART V - COMMUNICATIONS

	YES	NO
1. Is there more than one type of intercommunication equipment to use?	X	
2. Is adequate equipment available for spreading emergency alarms?	X	
3. Has the communication center been provided with special security safeguards?	REMARK	
4. Are security guards familiar with communication equipment in use?	X	
5. Is emergency power available for communication equipment?	X	
6. Is there a separate communication system for security personnel?	REMARK	
7. Is there a need for a separate guard communication system?	REMARK	

DA FORM 1 MAY 66 2806

Figure T-6—Example of completed inspection report (front of DA 2806).

PART VI - CRITICAL, VULNERABLE OR RESTRICTED AREA CONTROL

	YES	NO
1. Is there a separate physical security plan for this area?	X	
2. Is there a barrier around this area?	X	
3. Are there clear zones on both sides of the perimeter fence?	X	
4. Is protective lighting installed?	X	
5. Are anti-intrusion devices installed?	X	
6. Is there a need for anti-intrusion devices?	X	
7. Is there a system for personnel movement control?	X	

PART VII - EMERGENCY PLANNING

	YES	NO
1. Is there a mutual defense plan in existence with other military organizations stationed in the vicinity?	NA	
2. Are first aid and medical facilities available?	X	
3. Do emergency plans provide for personnel evacuation?	X	
4. Are personnel instructed to immediately report suspicious acts that may have to do with espionage or sabotage?	X	
5. Are security personnel trained for emergency operations?	X	
6. Do security personnel have additional duties of fire prevention?	X	
7. Is there a damage control plan in effect?	X	

PART VIII - MATERIAL AND EQUIPMENT STORAGE

	YES	NO
1. Are all storage and other secured buildings provided with adequate locking devices?	REMARK	
2. Are adequate protective measures afforded to open storage?	NA	
3. Is material in open storage properly stacked, placed within, away from, and parallel to perimeter barriers, in order to provide an unobstructed view by patrol personnel?	NA	
4. Are critical items such as weapons and ammunition stored in accordance with existing Army regulations?	REMARK	
5. Does the installation have a responsibility for shipment of classified material?	NA	
6. Are provisions made in the physical security plan for guards to be used to escort or guard classified material?	NA	

REMARKS AND COMMENTS

(See attached sheet)

RECOMMENDATIONS

(See attached sheet)

OVERALL EVALUATION OF PHYSICAL SECURITY

☐ EXCELLENT ☐ GOOD ☐ POOR Satisfactory

TYPED NAME, GRADE AND ORGANIZATION OF SURVEY OFFICER	SIGNATURE
Horace S. Bull, SFC, Office of the Provost Marshal, Ft Custer, OK	Horace S Bull

Figure T-6 Continued—Inspection report (back of DA 2806).

The results of physical security surveys and inspections must be documented. DA Form 2806, Physical Security Survey, is used for this purpose.

Form 2806 is divided into eight areas of concern in physical security inspections/surveys. The most involved portion of the form is usually the Remarks and Comments and Recommendations blocks on the reverse side. These two blocks often require attached sheets to fully reflect results. These portions are critical to the security manager or

Report No. 15-76

ANNUAL - UNANNOUNCED PHYSICAL SECURITY INSPECTION
AMMUNITION STORAGE POINT
FT CUSTER, OK 39999

Names of Individuals Interviewed:

Howard P. Platt, GS-5
Night Operations Supervisor

John N. Kelly, E4
Security Force Member

Names of Inspection Personnel:

William A. Cody, SSG, Physical Security Inspector,
Office of the Provost Marshal

MISSION: To receive, store and issue small arms ammunition in bulk lots for use in training and contingency missions for units located at Ft Custer, OK 39999.

Description of the Area:

The ammunition storage point is located on Big Horn Road and is the only ammunition storage area on the post. It covers twenty-four acres and has fourteen separate buildings. These buildings include twelve earth covered conventional ammunition storage igloos and two wooden administrative buildings. The storage area is surrounded by a thickly wooded area. The perimeter fence is a seven-foot, chain link with top guard. The perimeter has adequate protective lighting. (Include any information that would assist in preparation for future inspections.)

Recurring Deficiencies:

None

Remarks and Comments:

1. (Part II, Question 9) Security dog teams could be effectively employed in the ammunition storage area. As a result of a staff study directed by the Director of Industrial Operations, security dogs with handlers are on requisition and kennel facilities are under construction. (Key to items on Form 2806.)

Recommendation: None

Figure T-6 Continued—Inspection report (attached sheets).

installation commander, because the information here could be helpful in obtaining additional equipment and devices to properly accomplish the physical security mission. The information also may be helpful in budget and manpower requests (chapter 2).

2. (Part IV, Question 2) Many of the restricted area signs posting the perimeter have been removed or have fallen down. (Key to items on Form 2806.)

Recommendation: Missing signs should be replaced and many existing signs should be reinforced or repaired to provide the proper restricted area posting (para 3-9a, AR 190-11). (Specific regulatory guidance should accompany each recommendation to correct a deficiency.)

3. (Part V, Question 3) The guard force communication center is the post interior guard house. This guard house is manned around the clock with a minimum of one armed guard/radio operator. Access to the building is obtained through a single entrance controlled by an electrically operated lock. No other special safeguards are provided or deemed necessary.

Recommendation: None

4. (Part V, Questions 6 and 7) The entire interior guard force is on the same radio as the permanent ammunition storage point security guards. The net is separate from the military police net, but may be monitored by the military police desk sergeant. Due to this monitoring capability and the limited amount of traffic on the net, the current radio communications system is adequate. A single party land line to the guard house is also provided through several call boxes located throughout the ammunition storage point.

Recommendation: None

5. (Part VIII, Question 1) A master key is in existence for both gates and four of the igloo entrances. All employees have a copy of the master key to the gates.

Recommendation: All master key locks should be replaced with locks requiring separate keys. No master keys should be allowed in the system (para 3-7f, AR 190-11).

6. (Part VIII, Question 4) An inventory procedure has not been established for accountability of ammunition stored at the ammunition storage point.

Recommendation: That an inventory procedure be established to insure accurate accountability (para 3-3c, AR 190-11).

Supplemental Remarks and Comments:

The security at the ASP has improved significantly over the past year. The commander and security officer are to be commended for the upgrading to the present security posture.

Figure T-6 Continued—Inspection report (attached sheets).

Manpower survey reports describe work performed by various security force members. A yardstick (chapter 2, section V) can help to establish workload and performance data to justify existing or additional manpower needed to perform the security mission.

Completed forms should reflect at least the actual manhours expended, strength, and annual and sick leave factors. With the data indicated in the examples here and with reference to the DA Pam 140-series, your response to justification requirements should be much easier.

DATE OF REPORT	DATA AS OF	STATION AND ADDRESS (Include ZIP Code)	TDA DESIGNATION	REPORTS CONTROL SYMBOL CSFOR-76
13 Sep 1979	31 Jul 1979	Fort Madison, Iowa 52001	5A WZXYAA 00	

SECURITY OFFICE
ACTIVITY

MANPOWER SURVEY REPORT

For use of this form, see AR 570-4; the proponent agency is the Office of the Assistant Chief of Staff for Force Development.

COMPOSITION OF THE REPORT

DA Form 140 - GENERAL FORM (serves as cover sheet)
DA Form 140-1 - REMARKS
DA Form 140-2 - SCHEDULE A - MANPOWER INVENTORY
DA Form 140-3 - SCHEDULE T - IDENTIFICATION OF OTHER MANPOWER
DA Form 140-4 - SCHEDULE X - MANPOWER AND WORKLOAD DATA
DA Form 140-5 - SCHEDULE A - MANPOWER INVENTORY (Continuation Sheet)

NOTE:
This report is prescribed by AR 570-4, Manpower and Equipment Control - Manpower Management. Examples and detailed instructions for the preparation of this report are contained in DA Pamphlet 570-4, Manpower Procedures Handbook.

MAJOR COMMAND	TYPED NAME AND GRADE OF SURVEY TEAM CHIEF	SIGNATURE OF SURVEY TEAM CHIEF
TRADOC	DONALD Q. HEY, LTC, GS	/s/ Donald Q. Hey

DA FORM 1 DEC 73 140 — PREVIOUS EDITIONS OF THIS FORM ARE OBSOLETE. — GENERAL FORM

Figure T-7—Sample manpower survey report (cover, p. 1 of 35).

MANPOWER SURVEY REPORT - REMARKS For use of this form, see AR 570-4; the proponent agency is Office of the Assistant Chief of Staff for Force Development.	1. SHEET NO.	2. LINE NO.	REPORTS CONTROL SYMBOL CSFOR-76

3. CHECK APPLICABLE BLOCK. ☐ SURVEY TEAM GENERAL REMARKS *(complete item 4, only, and file after Commander's General Remarks.)*

☒ COMMANDER GENERAL REMARKS *(complete item 4, only, and file after Coversheet, DA Form 140.)*

☐ SURVEY TEAM SPECIFIC REMARKS *(If this block is checked, complete items 1, 2, and 4 and file with Schedule X.)*

4. REMARKS: *(If more space is required, continue on plain paper 10½" x 8".)*

1. Date of last manpower utilization survey: 18 January - 26 February 1978.

2. The general mission of the garrison is to maintain and operate the Fort Madison Military Reservation (FMMR) and administer, supply and service all units and activities located on this installation. Current mission statement is attached.

3. a. FMMR experiences an unusually large turnover of personnel because of its training mission. This turnover has a definite impact on workloads in the Adjutant General, Finance and Accounting, and installation housekeeping areas. Additional personnel in Finance and Accounting (pay and travel), Headquarters Commandant (temporary and permanent housing), and Special Services (recreational activities) are required because students make up a large percentage of the population.

b. The widely dispersed physical layout of FMMR covering 125,000 acres affects workloads in transportation (i.e., bus service for students), maintenance (especially aircraft maintenance which is accomplished in several widely dispersed areas), and fire protection.

4. a. Four hundred units of on-post housing are scheduled for completion between August 1980 and 1981. Additional workloads will materialize in areas of Engineer, Headquarters Commandant, Finance and Accounting (billing and collecting), Communication-electronics.

b. Auxiliary Field No. 4 is scheduled for completion 1 November 1981. In addition to staffing for this airfield, manpower increases will be required in the Aircraft Maintenance, Communications-electronics, and Engineer areas.

5. Manpower changes resulting from anticipated changes in workload are specifically indicated on the Schedules X for the activities concerned.

6. Improved manpower utilization would be possible if:

a. Higher headquarters reviewed required reports to insure staggered due dates, thereby permitting leveling off of reporting workload.

b. The commanders were provided greater flexibility in organizing the garrison,

FOR EXAMPLES AND INSTRUCTIONS, SEE APPENDIX B, DA PAMPHLET 570-4.

DA FORM 140-1 1 DEC 73 PREVIOUS EDITIONS OF THIS FORM ARE OBSOLETE. ☆ U.S. GPO: 1974—540-842/8623

Figure T-7 Continued—General remarks by the commander (p. 2 of 35).

MANPOWER SURVEY REPORT - REMARKS For use of this form, see AR 570-4; the proponent agency is DCSPER.	1. SHEET NO.	2. LINE NO.	REPORTS CONTROL SYMBOL CSFOR-76

3. CHECK APPLICABLE BLOCK. X SURVEY TEAM GENERAL REMARKS (complete item 4, only, and file after Commander's General Remarks.)
COMMANDER GENERAL REMARKS (complete item 4, only, and file after Coversheet, DA Form 140.)
SURVEY TEAM SPECIFIC REMARKS (If this block is checked, complete items 1, 2, and 4 and file with Schedule X.)

4. REMARKS: (If more space is required, continue on plain paper 10½" x 8".)

1. The current manpower survey was conducted during the period 1-13 Sep 79, by a team of seven members.

2. During the period of the survey, the population of the post was approximately 20,000; however, based upon general average population during the past year and current projections, the survey team recognized 26,000 as the military population workload basis for staffing. Other missions include operation of a US Army hospital (500 beds); operation of a regional engineer field maintenance shop; and support of numerous TRADOC activities located in the general vicinity of FMMR.

3. The overall factors affecting manpower requirements referred to by the commanding officer were taken into consideration by the survey team in the team's specific recommendations shown on Schedules X. In some cases special tolerances were recommended, particularly in the case of dispersal factors.

4. The remarks of the commander concerning anticipated changes in workload were considered by the survey team during survey of the respective activities concerned. Recommendations concerning manpower requirement adjustments are contained in survey team remarks on the separate Schedules X. It is pointed out that the full effect of new construction upon workloads of installation activities probably will not be felt until approximately midsummer of 1980. Manpower requirements for future workload increases must be determined at the time they actually develop.

5. The installation commander's remarks concerning the possibility of increased manpower utilization if staggered due dates of reports were established, is concurred in by the survey team. A review of required reports indicates that 75% of the 165 recurring reports submitted by FMMR have due dates during the first 10 days of each month. This creates an almost intolerable administrative burden which should be solved by higher headquarters.

FOR EXAMPLES AND INSTRUCTIONS, SEE APPENDIX B, DA PAMPHLET 570-4.

DA FORM 140-1, 1 DEC 73 — PREVIOUS EDITIONS OF THIS FORM ARE OBSOLETE.

☆ U.S. GPO: 1975—580-842/8429

Figure T-7Continued—Survey team's general remarks (p. 3 of 35).

MANPOWER SURVEY REPORT -SCHEDULE X - MANPOWER AND WORKLOAD DATA
For use of this form, see AR 570-4; the proponent agency is DCSPER.

REPORTS CONTROL SYMBOL CSFOR-76

MAJOR STAFF ELEMENT	DIVISION	BRANCH	SECTION OR UNIT	SHEET NO.	LINE NO.
Dir for Admin	Security	Ofc of Chief		8	4

DESCRIPTION OF WORK PERFORMED Provides advice and assistance to the Commander, staff, and subordinate commanders relative to physical and personnel security on the post, tenant units as assigned, and off-post activities. Plans, directs, and executes the Federal Personnel Security Program and the Intelligence Program to provide for the security of classified defense information, material, and post resources. Directs and administers the physical security program and Provost Marshal functions of the installation. Directs security police personnel

YARDSTICK CODE
a. 570-566-34.1
b. 12.2

WORK UNIT
a. Str of Sec Div
b. Total Post Str

SECTION A - SUMMARY OF MANPOWER

	OFF a	WO b	ENL c	US CIV d	NON-US CIV e	TOTAL MAN-POWER SUBJ TO ALLOC f	OTHER MANPOWER US g	OTHER MANPOWER NON-US h	TOTALS i
1. ALLOCATION	1			8		9			9
2. ACTUAL STRENGTH	1			10		11			11
3. RECM BY CO	1			12		13			13
4. RECM BY SURVEY TEAM	1			3		•4			4

YARDSTICK ALLOWANCE COMPUTATION

SECTION B - PERFORMANCE DATA

YEAR AND MONTH 19 78 - 79 a	MANPOWER: AVG STR b	MANPOWER: TOTAL MAN-HOURS WORKED c	MANPOWER: HRS OP IN MO d	MANPOWER: EQUIV MAN-MONTHS (c ÷ d) e	WORKLOAD: NO. OF WORK UNITS f	WORKLOAD: W/L PER PERSON (f ÷ e) g
SEP	9	1304	160	8.2	88	10.7
OCT	8	1229	168	7.3	88	12.1
NOV	8	1147	160	7.2	88	12.2
DEC	8	1134	168	6.8	89	13.1
JAN	8	1422	176	8.1	100	12.3
FEB	8	1239	152	8.2	98	12.0
MAR	9	1518	168	9.0	99	11.0
APR	9	1487	176	8.4	99	11.8
MAY	10	1519	168	9.0	95	10.5
JUN	12	1915	168	11.4	95	8.3
JUL	14	2273	176	12.9	96	7.4
AUG	14	2024	168	12.0	93	7.8

1. WORKLOAD USED AS BASIS OF APPRAISAL
2. AVERAGE PRODUCTIVITY
3. MANPOWER ALLOWANCE
SURVEY WORKLOAD (1) (____) / AVG PRODUCTIVITY (2) (____) = ____ × 1.11 = ____

SECTION C - MANPOWER

ALLOC STR a	RANK OR GRADE b	ACTUAL STR c	RANK OR GRADE d	JOB TITLE e
1	MP 03	1		Chief
1	GS 11	1		Security Off
1	GS 09	1		Investigator
1	GS 05	3		Guard
1	GS 05	1		Pers Sec Clk Steno
1	GS 04	1		Guard
		1	GS 04	Invest Stud Trainee
1	GS 04	1		Clk Gen Typ
1	GS 03	0		Clk Gen
1	GS 03	0		Clk Typ
		1	GS 01	Clk Gen Trainee
9		11		TOTAL

AMS CODE:

TDA PARA: 017

DA FORM 1 NOV 73 140-4 PREVIOUS EDITIONS OF THIS FORM ARE OBSOLETE.

Figure T-7 Continued—Schedule X, manpower, and workload data No. 1 (p. 4 of 35).

153-846 0 - 94 - 20

SECTION D - SPECIFIC REMARKS

COMMANDER

COMMANDER'S RECOMMENDED STAFFING

DIME'S CATEGORY	COVERABLE	COVERED
I		
II		
III	13	11
IV		

a. CHIEF OF SECURITY (Military - MAJOR) - The Chief of Security assigned FMMR has been assigned multiple duties which include, but are not limited to the following:

Provost Marshal - responsible for overall supervision and management of law enforcement, traffic control, crime prevention program, and all investigations.

Security Manager - Supervises the proper implementation of DOD Regulation 5200.1-R, DOD Information Security Program, AR 380-5, DA Information Security Programs; provides guidance and supervises the security awareness program.

Intelligence Officer - Supervises the personnel security program, screens all personnel investigation reports, authorizes access to classified defense information for the Commander, and is the Files Procurement Officer for all personnel security investigative files. The population of FMMR includes 4466 civilians and 66 military personnel.

Post Game Warden - Supervises the implementation of post and state regulations pertaining to fishing and hunting of wildlife within the confines of FMMR.

Chief, Security Division - Responsible for the overall supervision and management of all activities within the Security Division. This includes the issuance of decals for vehicle control, access badges for personnel control and visitor control to FMMR.

The Security Division is composed of 99 civilians. The FMMR comprises 15,214 acres and Smokey River Storage Depot comprises 3,009 acres. Within the confines of this installation there are thousands of small arms weapons and ammunition. Also, the chemical munitions mission requires rigid security controls and continuous planning for safeguarding this mission.

b. SECURITY OFFICER, GS-11. The Security Officer is responsible for the planning, organizing, coordinating and directing of the security program at this installation. Maintains continuity of program with the change of military Chief of Security. Directs through subordinate supervisors a guard force of 89 personnel. Conducts investigations of violations of physical security and/or of a criminal nature. During the past year the workload for this position has been extremely heavy due to constant change in physical security standards for safeguarding thousands of small arms weapons and ammunition. This post also has a chemical munition mission. Physical Security standards and requirements for the security of chemical munitions are more rigid than for

Figure T-7 Continued—(p. 5 of 35).

SECTION D - SPECIFIC REMARKS

COMMANDER

other munitions or weapons. The Security Officer is responsible for planning and organizing the security force for safeguarding property assigned this post. Has during the past year, revised security police orders, physical security plans and instructions for securing this post and property. The crime prevention program and plans have been reviewed and published and this involved many hours for research and planning. The supervision of three guard branches and one administrative section involved many hours and many problems. The continuous problems in safeguarding this installation and its property have also been time-consuming and have been a full-time job. The Security Officer serves as Deputy Provost Marshal, Alternate Security Manager, Alternate Intelligence Officer, Alternate Reservation Game Warden, Deputy Chief of Security, and as such, is responsible for the performance of duties during the absence of the Chief of Security. This position is considered essential to the accomplishment of the post mission and is fully justified.

The Security Officer provides technical assistance to Kaine Army Depot on all security related matters.

c. CIVILIAN INVESTIGATOR, GS-9. This position is essential to the accomplishment of the security mission and is a full-time job and justified. The majority of cases assigned the investigator are of a confidential nature and cannot be disclosed to the general public. All cases must be investigated promptly and they must be thorough and complete. Evidence collected must be factual and all cases must be brought to an intelligent conclusion. Many of the cases assigned the investigator involved missing weapons and ammunition. The investigation of this type case is time-consuming and is no easy task. The investigator has spent many hours on the phone and many more in the field checking clues, information, shipping documents, etc., to locate or account for missing weapons or ammunition and crimes of violence. Many hours are also required to prepare written reports of the shortages. Also considerable time is consumed in reporting missing weapons and ammunition and criminal cases to the FBI and CID personnel. In addition to the cases involving small arms weapons and ammunition, the investigator has investigated many incidents involving the loss or theft of missing sensitive and pilferable items such as expensive hand tools, air wrenches, drills, sanders, etc. These incidents have been a continuous problem and time-consuming in determining what happened to them.

During the period the following actions were accomplished:

Investigations of cases pertaining to crimes of violence crimes against property and complaints requiring investigation by investigator -------------------------- 46

Cases involving small arms, small arms ammo and buildings containing larger conventional ammo ---------- 35

Cases involving the loss or theft of sensitive and pilferable items and attempted theft of same -- 41

★ U.S. GPO: 1974—580-838/8048

Figure T-7 Continued—(p. 6 of 35).

Sheet 8 Line 4-1

DESCRIPTION OF WORK PERFORMED CONTINUED

engaged in protective activities to prevent pilferage, sabotage, and damage. Provides security guards and roving patrols for manning gates and guard posts, safeguarding classified material in transit, and patrolling warehouses and dependents' housing areas. Maintains liaison with Federal, state, and municipal law enforcement agencies.

Figure T-7 Continued—Continuation sheet (p. 7 of 35).

SECTION D - SPECIFIC REMARKS

COMMANDER

Physical security inspections, crime prevention surveys	888
SIRs	7
Assistance to off-post agencies	55

The requirement to conduct physical security inspections at this facility is not being fulfilled in a satisfactory manner based on the present workload requirement. There are 86 physical security inspections, including follow-ups, required at this installation annually, in addition to over 1000 igloos which must be inspected for physical security standards annually. Presently, the investigator is assigned to conduct these inspections and surveys in conjunction with the Crime Prevention Program as an added duty. The requirement to provide technical supervision at Kaine Army Depot in the area of physical security is also an additional duty assigned the investigator. Two additional personnel are needed to provide additional expertise to insure all standards and inspections required are met.

At present, an Investigator Student Trainee, GS-4, is being utilized to assist the investigator in the performance of these additional duties, but much valuable time is consumed in training this type help due to the fact that they only work 3 months at a time. Many of the duties cannot be performed by the trainee because of the nature of the incident and the knowledge required to effectively complete actions required.

The investigator trainee assisted the investigator in the following actions:

687 physical security inspections performed on igloos
23 investigations of complaints, larcenies, etc.

d. PERSONNEL SECURITY CLERK (STENO), GS-5 - This position is essential to the Security Division Personnel Security Program and is a full-time job. Some of the duties and responsibilities accomplished by the personnel security clerk during the past year are as follows:

During the period, the Personnel Security Clerk assisted the Security Manager/Intelligence Officer in performing the following actions:

Dossier reviews	19	Security clearances verified by telephone on Travel Orders	1260
Initial clearances	213	Security clearances verified by telephone on teletypes going off post	800
Clearances restored	65	Security clearances verified by telephone on visitors to this post	225
Request for investigations	40	Security clearances verified by telephone and written communications on post personnel	125
Clearances downgraded	10		
Debriefings	101		
Actions on sensitive positions	833		
Number of security inspections	38		

★ U.S. GPO: 1973—540-841/8543

Figure T-7 Continued—(p. 8 of 35).

SECTION D - SPECIFIC REMARKS

COMMANDER

NACI suitability investigations	501	Inquiries submitted to police department and law enforcement agencies for investigative purposes	110
Clearances terminated	148	Security orientations to newly assigned personnel (group presentation consisting of personnel for total from groups)	325
Acceptance of clearances issued by other posts	21		

Because of the multiple duties of the Chief of Security, it is necessary for the Personnel Security Clerk to do much of the "leg work" for the chief in carrying out the Personnel Security Program such as administering security tests for all personnel assigned to sensitive positions; preparing Security Awareness Orientation briefing material for all post personnel; screening Official Personnel Folders for compliance with personnel security investigations; security violations, spot intelligence reports, maintaining current status of each post employee's security status; preparing local supplements to DA and DOD regulations pertaining to Personnel Security/Intelligence, etc. In addition must give personnel security technical support to (Tenant Activities) FMMR Dispensary, USACC Detachment, Defense Property Disposal Office and (Detachment) Kaine Army Depot. Performs stenographic duties as required.

e. CLERK TYPIST, GS-3 AND CLERK GENERAL, GS-3 - These positions are assigned to Badge and Vehicle Identification to handle the badging of personnel and registration or privately-owned vehicles on a 40-hour per week basis, which requires services of two full-time employees. A Clerk General (Trainee) GS-1 is occupying the GS-3 Clerk General position. At times two additional employees are borrowed from within the division to process the volume of personnel. This causes much backlog in the offices from which these two personnel are borrowed.

During the period the following actions were processed:

Badges issued	2816	Parking tickets	404
Badges repaired	612	Laminations (other than badges)	978
Lost badges issued	198	Pet registrations	16
Fingerprints	1925	Weapons registrations	64
Fishing licenses	308	Radio permits	21
Special passes	339	Match permits	74
Separations	626	Decals issued to military	148
Parking permits	258	Decals issued to civilians & contractors	2962
ID cards	166	Decal terminations, military	80
Badges destroyed	472	Decal terminations, civ & contr	1864

☆ U.S. GPO: 1973—540-841/8543

Figure T-7 Continued—(p. 9 of 35).

SECTION D - SPECIFIC REMARKS

COMMANDER

Many hours are required daily, weekly and monthly answering the telephone, locating personnel, searching files and giving information. The 4466 civilian employees, 92 attached personnel, 66 military and their dependents assigned this post, plus the approximately 9000 civilian vehicles registered requires many hours weekly to maintain the files and records and is more than the Clerk Typist and Clerk General (Trainee) can handle and additional help frequently from other security personnel is required.

f. CLERK GENERAL (TYPING), GS-4 - This position is essential to the Security Division Physical Security Program and Security Division Administration and is a full-time job. Assists the Chief Security Division and Deputy Chief Security Division in all phases of the Physical Security Program such as preparation of Physical Security Plans, Guard Orders, Crime Prevention Plans, and Guard Handbook. Prepares local regulations and supplements regarding Motor Vehicle Traffic Supervision and Entry and Exit Controls. This involves reading appropriate ARs and AMCRs to assure that controls are in accordance with these regulations. Serves as the Training Officer for all security personnel on forms and administration within the division. Maintains driver record files on all post employees who have had violations. Maintains case files on all installation employees who have in the past been involved in fights, security violations, crimes against property, and crimes of violence, etc. Assists the investigator in the investigation of incidents as listed above. Staffs all Serious Incident Reports and Minor Incident Reports for submission to Department of the Army and US Army Materiel Command, etc., for this installation. Serves as the Reports Control Officer for the Security Division. Confers with key personnel to determine staffing requirements and personnel assignments to insure that manpower is properly and efficiently utilized at all times. Prepares overtime justifications as required. Serves as Organization Supply Officer and as such maintains all records for division equipment and property. Is responsible for the handling and controlling of all Security Division property valued at approximately $75,000. Performs the physical inventory of all property annually and periodically as required. Prepares supply transaction documents including requisitions, issues, turn-ins and any other actions affecting equipment. Helps in the preparation of justifications for capital and non-capital equipment.

Provides technical assistance to Shift Commanders, Shift Lieutenants, and all security personnel in the preparation of reports of investigations of incidents and accidents. As required, searches female personnel and women's restrooms for evidence in connection with official investigations or theft of Government property.

Actively participates in the development of plans and procedures consistent with appropriate security regulation and requirements to provide an adequate security program relative to all phases of Security Division activities. Makes work assignments to employees of lower grade engaged in clerical and typing duties, gives general instructions on procedures to be followed, resolves problems, spot checks routine work and reviews other work for accuracy, and as such, has supervisory responsibility over these operations, reporting directly to the Deputy Chief of Security.

* U.S. GPO: 1973—540-841/8543

Figure T-7 Continued—(p. 10 of 35).

SECTION D - SPECIFIC REMARKS

COMMANDER

Maintains control list for installation personnel authorized entrance into the Chemical Limited/Controlled Area. Reviews files assuring that all requirements and qualifications are met and maintained IAW FMMR regulations, ARs, and other directives. Requests toxic physicals, CHEs, and/or toxic training for all individuals as per category requirements. Submits requests for additions through proper channels to Security Officer or Commander as appropriate, for final approval. Coordinates with Surety Officer on changes in requirements.

Analyzes data, reviews requirements for budget and personnel and prepares divisional budget (within the division five separate budgets are prepared because of separate operational code costs) for submission to director. Selects historical data from division files and records and submits to the directorate for preparation of annual historical summary.

Because of the varied duties and responsibilities of the position, it is difficult to prepare a numerical report for actions completed at a given time. Some of the actions that are capable of being recorded as such are as follows:

For period Jul 77 through Jul 78:

Armed forces traffic tickets	75	Weapons authorizations	550
Accident investigations	31	Assistance rendered to local law enforcement personnel	90
Traffic violation warnings	50	Reviews of records for toxic suitability:	
Notifications to individuals that driving privileges were in jeopardy	10	Training records screened	300
		Medical records screened	300
SIRs	7	Telephone complaints	600
MIRs	2	Budgets prepared:	
MPRs	216	Initial	5
Information MPRs	995	Supplements	20
Blotters	365	Awards prepared	30
Off-post submissions	240	File checks	500
Personnel actions	80	File checks for CSC	105

g. CLERK GENERAL (TYPING), GS-3 - This position is assigned the Administrative Section and is essential to the operations of the Security Division and is a full-time job.

Performs typing duties, receives telephone calls, receives incoming mail and opens for review of supervisors. Maintains adequate supply of office supplies and blank forms for use by personnel of division. Initiates work rosters and training schedules. Prepares quarterly uniform vouchers for pay allowance for all guards on appropriate dates. Maintains office files in accordance to subject matter, chronological and numerical

★ U.S. GPO: 1973—540-841/8543

Figure T-7 Continued—(p. 11 of 35).

SECTION D - SPECIFIC REMARKS

COMMANDER

sequence. Maintains current reference material such as ARs, TMs, FMs, AMCR, and other directives. Serves as Alternate Reports Control Officer and Files Management Clerk with responsibility for sorting and preparing records for periodic shipment to RHA according to distribution schedules provided in regulations.

Prepares time and attendance reports. Assists the Clerk General (Typing), GS-4, in preparation of reports, filing, preparation of investigation reports, etc.

Because of the variety of duties associated with this position, it is difficult to include all duties as such. The time required to type reports and maintain files in the Security Division is enormous and requires two full-time employees.

Performs duties of Clerk General (Typing), GS-4, during absence of incumbent.

Recommend approval of 13 spaces.

★ U.S. GPO: 1973—540-841/8543

Figure T-7 Continued—(p. 12 of 35).

SECTION D - SPECIFIC REMARKS

COMMANDER

Summary of actual manhours, leave computation and recap of authorized and recommended spaces by AMS codes follows:

ACTUAL MANHOURS (Survey Period)	
Borrowed	
Loaned	
Overtime	425
Annual Lv	1337
Sick Lv	243
Other Lv	306
Civ TDY	
Mil Lv	192

LEAVE FACTOR

1. Actual Strength, Aug 77 (civ + mil) = 11 (pers) A
2. Sick leave, 62 X A = 682 (hrs) B
3. Annual Leave
   - CAT 8 (incl mil) 208 X 6 = 1248 (hrs)
   - CAT 6 160 X 3 = 480 (hrs)
   - CAT 4 104 X 2 = 208 (hrs)
   - SUM OF 3 = 1936 (hrs) C
4. Nonproductive leave time B + C = 2618 (hrs) D
5. Available time, 2008 X A = 22088 (hrs) E
6. Productive time, E - D = 19470 (hrs) F
7. Leave factor, D ÷ F + 1.00 = 1.13 G
8. % leave rate = D ÷ E X 100 = 12 %

AMS RECAP:

AMS CODE	ALLOC STR FTP	ALLOC STR TPT	ALLOC STR OFF	ALLOC STR ENL	ALLOC STR TOT	RECOMD BY COMD FTP	RECOMD BY COMD TPT	RECOMD BY COMD OFF	RECOMD BY COMD ENL	RECOMD BY COMD TOT
36AHG	2				2	4				4
36AHN	6		1		7	8		1		9

U.S. GPO: 1973—840-841/8843

Figure T-7 Continued—(p. 13 of 35).

MANPOWER SURVEY REPORT - REMARKS For use of this form, see AR 570-4; the proponent agency is Office of the Assistant Chief of Staff for Force Development.	1. SHEET NO. 8	2. LINE NO. 4-9	REPORTS CONTROL SYMBOL CSFOR-76

3. CHECK APPLICABLE BLOCK. ☐ SURVEY TEAM GENERAL REMARKS *(complete item 4, only, and file after Commander's General Remarks.)*

☐ COMMANDER GENERAL REMARKS *(complete item 4, only, and file after Coversheet, DA Form 140.)*

☐ SURVEY TEAM SPECIFIC REMARKS *(If this block is checked, complete items 1, 2, and 4 and file with Schedule X.)*

4. REMARKS: *(If more space is required, continue on plain paper 10½" x 8".)*

a. The Survey Team recommends 1 military and 3 civilian spaces for a total of 4 positions for this activity

b. Recommendation is based on governing survey rationale presented in Survey Team General Remarks.

c. Other considerations included:

(1) Letter AMCSS, 27 March 1974, subject, "Reorganization of AMC Security Offices".

(2) Change 1, DA Pam 570-566, Sept 1976, Table 566-34.1, 34.2, 34.3.

(3) AR 190-13, The Army Physical Security Program, 1 October 1976.

d. The Survey Team recommends reorganization of the Security Division to comply with AMC standard security staff organization consisting of one Security Office in the Directorate for Administration composed of three subordinate elements - Provost Marshal, intelligence and security guards.

e. The Survey Team recommends one civilian space to perform overall administrative management and budget planning functions for the Security Office.

f. The Survey Team recognizes one chief for overall management and control and one clerk-typist for clerical support.

g. The Survey Team recommends one civilian space for position of Deputy Security Officer. This space is recognized to provide essential stability and continuity of overall security operations and also provide dual responsibility as chief of Intelligence and Investigation Branch.

h. The recommended realinement of the Security Office will enable the Security Officer to evaluate workload and assign priorities to each function performed. The Security Officer will be in a position to delegate security programs organizationally and obtain better resource control than that experienced through vertical management.

FOR EXAMPLES AND INSTRUCTIONS, SEE APPENDIX B, DA PAMPHLET 570-4.

DA FORM 1 DEC 73 140-1 PREVIOUS EDITIONS OF THIS FORM ARE OBSOLETE.

* U.S. GPO: 1974—540-842/8623

Figure T-7 Continued—Remarks (p. 14 of 35).

MANPOWER SURVEY REPORT - SCHEDULE X - MANPOWER AND WORKLOAD DATA

For use of this form, see AR 570-4; the proponent agency is the Office of the Assistant Chief of Staff for Force Development.

REPORTS CONTROL SYMBOL CSFOR-76

MAJOR STAFF ELEMENT	DIVISION	BRANCH	SECTION OR UNIT	SHEET NO.	LINE NO.
Dir for Admin	Security	Security No. 1,2,&3	SUMMARY	8	4-a

DESCRIPTION OF WORK PERFORMED

Develops, implements, and enforces traffic regulations and maintains security of the installation.

YARDSTICK CODE: 570-566-34.3

WORK UNIT: Posts & Patrols

SECTION A - SUMMARY OF MANPOWER

	OFF a	WO b	ENL c	US CIV d	NON-US CIV e	TOTAL MAN-POWER SUBJ TO ALLOC f	OTHER MANPOWER US g	OTHER MANPOWER NON-US h	TOTALS i
1. ALLOCATION				(91)		(91)			(91)
2. ACTUAL STRENGTH				(82)		(82)			(82)
3. RECM BY CO				(96)		(96)			(96)
4. RECM BY SURVEY TEAM				(94)		(94)			(94)

YARDSTICK ALLOWANCE COMPUTATION

SECTION B - PERFORMANCE DATA

YEAR AND MONTH 19 76/77	MANPOWER: AVG STR b	TOTAL MAN-HOURS WORKED c	HRS OP IN MO d	EQUIV MAN-MONTHS (c ÷ d) e	WORKLOAD: NO. OF WORK UNITS f	W/L PER PERSON (f ÷ e) g
SEP	85	13082	160	81.8		
OCT	84	13614	168	81.0		
NOV	85	13378	160	83.6		
DEC	84	13682	168	81.4		
JAN	90	16230	176	92.2		
FEB	95	14959	152	98.4		
MAR	94	15699	168	93.5		
APR	88	15530	176	88.2		
MAY	90	15443	168	91.9		
JUN	85	13552	168	80.7		
JUL	86	14483	176	82.3		
AUG	82	13295	168	79.1		

1. WORKLOAD USED AS BASIS OF APPRAISAL

2. AVERAGE PRODUCTIVITY

3. MANPOWER ALLOWANCE

SURVEY WORKLOAD (1) ( ) / AVG PRODUCTIVITY (2) ( ) = ____ × 1.11 = ____

SECTION C - MANPOWER

ALLOC STR a	RANK OR GRADE b	ACTUAL STR c	RANK OR GRADE d	JOB TITLE e

AMS CODE:

TDA PARA:

DA FORM 1 NOV 73 140-4

PREVIOUS EDITIONS OF THIS FORM ARE OBSOLETE.

Figure T-7 Continued—Workload data No. 2 (p. 15 of 35).

SECTION D - SPECIFIC REMARKS

COMMANDER

COMMANDER'S RECOMMENDED STAFFING

DIME'S CATEGORY	COVERABLE	COVERED
I		
II	SEE INDIVIDUAL SCHEDULES	X
III		
IV		

Within the three Security Branches, there are 6 supervisors who are not included in the manning for the posts and patrols listed below:

POST		NO. PERS REQUIRED
Radio Room, 24-hour post, 7 days per week (permanent operators assigned)		6.0
Brown Gate, 1530-0710 hrs, Mon-Fri, 24 hours Sat, Sun, and Holidays		3.2
Coosa Avenue Gate, 24-hour post, 7 days per week		4.8
Eulaton Gate, 24-hour post, 7 days per week		4.8
Visitors Check Point, 8-hour post, 5 days per week (2-man post)		2.2
Post 12, entrance to Chemical Area, 8-hour post, 5 days per week (2-man post)		2.2
	Total	23.2

PATROLS		
Car 11 - 24-hour patrol, 7 days per week		4.8
Car 12 - 24-hour patrol, 7 days per week		4.8
Car 13 - 24-hour patrol, 7 days per week		4.8
Car 13A - 24-hour patrol, 7 days per week		4.8
Car 14 - 24-hour patrol, 7 days per week		4.8
Car 15 - 24-hour patrol, 7 days per week		4.8
Car 16 - 24-hour patrol, 7 days per week		4.8
Car 16A - 24-hour patrol, 7 days per week		4.8
Car 17 - 24-hour patrol, 7 days per week		4.8
Car 17A - 24-hour patrol, 7 days per week		4.8
Car 18 (Security Alert Team) - 24-hour patrol, 7 days per week (2-man patrol)		9.6
Car 19 - 24-hour patrol, 7 days per week		9.6
	Total	67.2
Six supervisors	Total	6.0
	Grand Total	96.4

★ U.S. GPO: 1973—540-841/8543

Figure T-7 Continued—(p. 16 of 35).

SECTION D - SPECIFIC REMARKS

COMMANDER

GUARD SUPERVISOR, GS-8 and GS-7 - There are currently six supervisors authorized the guard force - two supervisors per each 8-hour shift. The ratio of supervisory personnel to security personnel is determined by the individual characteristics of each installation. There must be as a minimum, a sufficient supervision to enable the inspection of each post and patrol twice per shift plus sufficient reserve to provide for sick and annual leave. Supervisory personnel cannot be determined by staffing guides for post manning. The ratio of police supervisory personnel at this depot is considerably less than the minimum essential requirements. The stationary post and motor patrols providing security control and coverage for the FMMR's 15,214 acres and the CRSA's 3,009 acres are from 1 to 5 miles apart and the CRSA is 13 miles from FMMR. The minimum inspection of each post and patrol twice each shift can be accomplished when both supervisors are present, but cannot be made at other times. The two supervisors are on duty together only three days per week at the most. The supervision of a guard force composed of from 28 to 30 men is a full-time job and involves many duties and responsibilities. The training of security personnel are among these essential responsibilities. Security Standards require all security personnel to complete a basic training course of in-service and advanced training in order to assure continued proficiency and development. Supervisors are responsible for conducting the training. The installation's chemical mission also requires constant training for security personnel. Many hours are spent each week on the job and in the field training security personnel in handling incidents and safeguarding chemical munitions. This training is mandatory and with any less than two supervisors per shift, this could not be accomplished and security personnel would not be qualified or capable of performing the chemical munitions security mission. Supervisors are alsc responsible for accident investigation which occur daily, also complaints and report writing and many other duties during their tour of duty. Supervisors, two per shift, are essential to the accomplishment of the security mission and are fully utilized and justified.

Radio Room is the Desk Control for FMMR security police. He has control over the dispatching and receiving of complaints and vehicle response to accidents/incidents. He maintains continual contact with all mobile patrols and keeps the shift supervisor informed of any incidents of an unusual nature. He provides for the initial notification of personnel to staff the Emergency Control Center in the event of an emergency.

Brown Gate is the main entrance to FMMR during non-regular duty hours. All incoming and outgoing traffic is processed in accordance with post regulations, visitor control and cargo carrying vehicle procedures. The purpose is to meet, greet and maintain full control of all authorized pedestrian and vehicular traffic to prevent unauthorized entry and to detect individuals intent upon entry for the purpose of sabotage, espionage, or other illegal acts.

Coosa Avenue Gate is the main entrance to the Ammunition Limited Area. This post is responsible for controlling authorized entry and exit for a properly designated limited area, to enforce all vehicular and pedestrian safety and security regulations, to preclude access by unauthorized persons and those individuals intent upon entry for sabotage, espionage or other illegal acts.

* U.S. GPO: 1973-540-841/8543

Figure T-7 Continued—(p. 17 of 35).

SECTION D - SPECIFIC REMARKS

COMMANDER

Eulaton Gate is the only access to the installation on the eastern boundary and is responsible for meeting, greeting, and maintaining full control of all vehicular and pedestrian traffic to preclude unauthorized access by persons intent upon sabotage, espionage or other illegal acts. It is also used to process employees into and out of the post. Eulaton Gate is located at the east entrance to the installation and only a short distance (approx. 2 blocks) from the large industrial center, maintenance rebuild shops, small arms weapons rebuild shops, small arms weapons storage and classified storage buildings. The East Area covers 650 acres and this is patrolled. The security personnel on duty at the Eulaton Gate on a full-time basis, provides security in depth and is certainly a justifiable deterrent for the protection of the thousands of small arms weapons stored in this area. Persons off duty are continuously being called in to work to make emergency repairs to expensive machinery and during electrical power interruptions which are on a daily basis, many times two or more during non-work hours. This entrance is the most direct route to the scene of these machines and emergencies and costly valuable time would be wasted for repair crews to enter and leave through the Brown Gate located approx. 5 miles from the East Area. This would increase the cost to the government and would be considerably more than the cost involved in operating this post 24 hours, 7 days per week. This gate entrance is also the most direct entrance point for military alert forces and EOD teams from Ft Ochs, assigned the responsibility of reporting to this installation in the event of chemical munitions incidents. Because of high priority given security of tanks, other armored vehicles and small arms and ammunition, patrols could not be called to man this gate during emergency situations as a lack of total security would exist. Several shifts have been added in this area and employees are working around the clock. Also, contractor personnel use this entrance, and because of the large number of contracts recently, this gate is used more than ever. The additional cost to these personnel by having them travel additional miles to another entrance to their work sites, is unreasonable.

Visitor's Check Point - is the main entrance to the post for all vehicular and pedestrian traffic during normal operational hours. Outgoing traffic is searched and inspected to determine that only authorized property is being removed from the post. Two men are required to operate this post on an 8-hour, 5-day per week basis.

Post 12 - is the entrance to the Chemical Area and is responsible for controlling pedestrian and vehicle access to the area; for assuring that entry is authorized by competent authority and that all regulations and orders pertaining to safety and security are met prior to entry even when authorized. Two-man rule for this area is mandatory, IAW regulations.

Cars 11, 13, and 13A are responsible for the patrolling of the installation controlled areas, including all structures, warehouses, and operating facilities within these areas that are designated limited areas requiring periodic checks and inspections. These mobile radio patrols are also responsible for preventing loss and the surreptitious entry to government buildings for the detection of forced entry to government property, enforcement of traffic regulations, law and order for the protection of individuals working and/or living on the

* U.S. GPO: 1973—540-841/8843

Figure T-7 Continued—(p. 18 of 35).

SECTION D - SPECIFIC REMARKS

COMMANDER

installation. Provides money escorts. Car 13A has been added due to the high priority given security to tanks and other armored type vehicles located in the East Area of the installation, by the Special Study Group. This patrol further provides security to small arms weapon storage area.

Cars 12, 14, 15, 17 and 17A are mobile patrols responsible for patrolling within the Ammunition Limited Area. They have responsibility for preventing loss and surreptitious entry to government buildings and property, enforcement of traffic regulations, law and order for the protection of individuals working. For using special skills and training in providing for the protection, inspection, and in the event of emergencies, special actions with regards to the storage of all types of ammunition, explosives, and related materials. Additionally, assists in chemical related accident/incidents. Car 17A was added in order to provide additional security to G-block, Lance Missile complex and perimeter security to the North and Northwest section of the installation.

Cars 16 and 16A are assigned responsibility for the Smokey River Storage Annex. Car 16A was added on a 24-hour per day, 7-day-per-week basis to provide additional security at Coosa because CRSA is an ammunition limited area consisting of 136 storage igloos and over 3,000 acres. This area is in an isolated area and is located 13 miles from the FMMR.

Car 18 is designated as the Security Alert Team and is responsible for responding to an incident chemically-related anywhere on the post within 10 minutes, properly equipped and capable of responding regardless of the situation. They have been given an area of patrol which is designed to augment a patrol currently responsible for the area, therefore allowing them to respond without vacating an area of responsibility, and requires two men.

Car 19 is the patrol assigned responsibility for patrolling the confines of the Chemical Limited Area. They have total responsibility for providing security, enforcing traffic laws and orders, and regulations. Because of the sensitivity of the area patrolled and regulatory requirements, this patrol is a two-man patrol.

The increase in patrols was initiated as part of the recommendations proposed by the DA Special Study Group to upgrade the security posture. The report of this Special Study Group can be reviewed in the Classified Document Custodian's Office.

Many spaces will be required in addition to the spaces requested herein, as soon as the revised ARs 190-3 and 190-11 are placed into effect, due to more stringent and strict security controls.

Recommend approval of 96 spaces.

* U.S. GPO: 1973—540-841/8843

Figure T-7 Continued—(p. 19 of 35).

MANPOWER SURVEY REPORT - REMARKS
For use of this form, see AR 570-4; the proponent agency is DCSPER.

1. SHEET NO. 8 | 2. LINE NO. 4-a-4 | REPORTS CONTROL SYMBOL CSPOR-76

3. CHECK APPLICABLE BLOCK. ☐ SURVEY TEAM GENERAL REMARKS (complete item 4, only, and file after Commander's General Remarks.)
☐ COMMANDER GENERAL REMARKS (complete item 4, only, and file after Coversheet, DA Form 140.)
☐ SURVEY TEAM SPECIFIC REMARKS (If this block is checked, complete items 1, 2, and 4 and file with Schedule X.)

4. REMARKS: (If more space is required, continue on plain paper 10½" x 8".)

a. The Survey Team recommends 94 civilian spaces for this activity.

b. Recommendation is based on governing survey rationale presented in Survey Team General Remarks.

c. Other considerations included:

(1) On-site review of workload projections and priorities.

(2) Past utilization 95.6 or 96 manyears.

(3) Sick leave usage of 6812 hours is considered excessive and above DA norm. High rate of sick leave was primarily due to two employees on prolonged sick leave awaiting processing of papers for retirement.

(4) Overtime usage of 19,949 hours was excessive. Excessive turnover of personnel resulted in continuous personnel turbulence which is reflected in usage of excessive overtime.

(5) Recommended space for this branch was recognized on a consolidated basis.

d. Recommended staffing is based on an examination of each post and patrol recommended by the Commander, regulatory requirements for special security, safety considerations, DA 570-566-34.3 and past utilization.

e. Following is a list of posts and patrols recognized by the Survey Team:

Post/Patrols	Days Per Week	Hours	Guards	Manpower Allowance
Radio Room	7	24	1	4.8
Brown Gate (M-F)	5	16	1	
Brown Gate (S-S)	2	24	1	
Brown Gate (Holidays)	(9)	8	1	3.7
Coosa Avenue Gate	5	13	1	2.2
Eulaton Gate	7	24	1	4.8
Visitors Check Point	5	8	2	2.3
Post 12 (Chem Area)	5	8	2	2.3

FOR EXAMPLES AND INSTRUCTIONS, SEE APPENDIX B, DA PAMPHLET 570-4.

DA FORM 140-1, 1 DEC 73 — PREVIOUS EDITIONS OF THIS FORM ARE OBSOLETE.

★ U.S. GPO: 1975—580-842/8429

Figure T-7 Continued—(p. 20 of 35).

MANPOWER SURVEY REPORT - REMARKS
For use of this form, see AR 570-4; the proponent agency is DCSPER.

1. SHEET NO.	2. LINE NO.	REPORTS CONTROL SYMBOL
8	4-a-5	CSFOR-76

3. CHECK APPLICABLE BLOCK. [ ] SURVEY TEAM GENERAL REMARKS (complete item 4, only, and file after Commander's General Remarks.)
[ ] COMMANDER GENERAL REMARKS (complete item 4, only, and file after Coversheet, DA Form 140.)
X SURVEY TEAM SPECIFIC REMARKS (If this block is checked, complete items 1, 2, and 4 and file with Schedule X.)

4. REMARKS: (If more space is required, continue on plain paper 10½" x 8".)

Post/Patrols	Days Per Week	Hours	Guards	Manpower Allowance
Patrol 11	7	24	1	4.8
Patrol 12	7	24	1	4.8
Patrol 13	7	24	1	4.8
Patrol 13A	7	24	1	4.8
Patrol 14	7	24	1	4.8
Patrol 15	7	24	1	4.8
Patrol 16	7	24	1	4.8
Patrol 16A	7	24	1	4.8
Patrol 17	7	24	1	4.8
Patrol 17A	7	24	1	4.8
Sat 18	7	24	2	9.6
Chemical Area Patrol 19	7	24	2	9.6
			TOTAL	87.7
			Six Supervisors	6.0
				93.7

f. Brown Gate is open when Visitors Check Point Gate is closed, i.e., Mondays-Fridays 1530 hours to 0710 hours; 24 hours, Saturdays, Sundays, and Holidays.

g. Coosa Avenue Gate is being operated 13 hours a day, five days a week.

h. Ten additional spaces for increased patrol were allocated this activity as a result of recommendations to the Commander by the DA Special Study Group, June, 1977. The report of this special study group is classified and on file in the Classified Document Custodian's Office.

FOR EXAMPLES AND INSTRUCTIONS, SEE APPENDIX B, DA PAMPHLET 570-4.

DA FORM 1 DEC 73 140-1 PREVIOUS EDITIONS OF THIS FORM ARE OBSOLETE. * U.S. GPO: 1975—880-842/8429

Figure T-7 Continued—(p. 21 of 35).

MANPOWER SURVEY REPORT -SCHEDULE X - MANPOWER AND WORKLOAD DATA
For use of this form, see AR 570-4; the proponent agency is the Office of the Assistant Chief of Staff for Force Development.

REPORTS CONTROL SYMBOL CSFOR-76

MAJOR STAFF ELEMENT	DIVISION	BRANCH	SECTION OR UNIT	SHEET NO.	LINE NO.
Dir for Admin	Security	Security Br No. 1		8	5

DESCRIPTION OF WORK PERFORMED

Develops, implements, and enforces traffic regulations and maintains security of the installation.

YARDSTICK CODE: 570-566-34.3

WORK UNIT: Posts & Patrols

SECTION A - SUMMARY OF MANPOWER

	OFF a	WO b	ENL c	US CIV d	NON-US CIV e	TOTAL MAN-POWER SUBJ TO ALLOC f	OTHER MANPOWER US g	OTHER MANPOWER NON-US h	TOTALS i
1. ALLOCATION					31	31			31
2. ACTUAL STRENGTH					28	28			28
3. RECM BY CO					32	32			32
4. RECM BY SURVEY TEAM					32	32			32

YARDSTICK ALLOWANCE COMPUTATION

SECTION B - PERFORMANCE DATA

YEAR AND MONTH 19 77 /78	MANPOWER: AVG STR b	TOTAL MAN-HOURS WORKED c	HRS OF IN MO d	EQUIV MAN-MONTHS (c ÷ d) e	WORKLOAD: NO. OF WORK UNITS f	W/L PER PERSON (f ÷ e) g
SEP	29	4411	160	27.6		
OCT	29	4916	168	29.2		
NOV	28	4532	160	28.3		
DEC	27	4529	168	27.0		
JAN	30	5583	176	31.7		
FEB	32	5185	152	34.1		
MAR	32	5418	168	32.3		
APR	30	5383	176	30.6		
MAY	30	5187	168	30.9		
JUN	29	4603	168	27.4		
JUL	31	5196	176	29.5		
AUG	28	4502	168	26.8		
1. WORKLOAD USED AS BASIS OF APPRAISAL						
2. AVERAGE PRODUCTIVITY						

3. MANPOWER ALLOWANCE

SURVEY WORKLOAD (1) ( ) / AVG PRODUCTIVITY (2) ( ) = ______ × 1.11 = ______

SECTION C - MANPOWER

ALLOC STR a	RANK OR GRADE b	ACTUAL STR c	RANK OR GRADE d	JOB TITLE e
1	GS-08	1		Guard Supv
1	GS-07	1		Guard Supv
12	GS-05	11		Guard
13	GS-04	13		Guard
	GS-03	2		Guard
(27)		(28)		
TEMP	SPACES	SUBJ TO	AUTH	
4	GS-04			Guard
(4)				
SEE SURVEY TEAM REMARKS SHEET 8, LINE 4a FOR RATIONALE LEADING TO RECOMMENDED STAFFING.				
31		28		TOTAL

AMS CODE: 36AHG

TDA PARA: 017A

DA FORM 1 NOV 73 140-4 PREVIOUS EDITIONS OF THIS FORM ARE OBSOLETE.

Figure T-7 Continued—Workload data No. 3 (p. 22 of 35).

SECTION D - SPECIFIC REMARKS

COMMANDER

COMMANDER'S RECOMMENDED STAFFING

DIME'S CATEGORY	COVERABLE	COVERED
I		
II		
III	32	28
IV		

★ U.S. GPO: 1973—540-841/8543

Figure T-7 Continued—(p. 23 of 35).

SECTION D - SPECIFIC REMARKS

COMMANDER

Summary of actual manhours, leave computation and recap of authorized and recommended spaces by AMS codes follows:

ACTUAL MANHOURS (Survey Period)		LEAVE FACTOR			
Borrowed		1. Actual Strength, Aug 77 (civ + mil)		= 28 (pers)	A
Loaned		2. Sick leave, 62 X A		= 1736 (hrs)	B
Overtime	6145	3. Annual Leave			
Ann Lv	4894	CAT 8 (incl mil)	208 X 17 = 3536 (hrs)		
Sick Lv	746	CAT 6	106 X 11 = 1760 (hrs)		
Other Lv	384	CAT 4	104 X = ____ (hrs)		
Civ TDY		SUM OF 3		= 5296 (hrs)	C
Mil Lv		4. Nonproductive leave time B + C		= 7032 (hrs)	D
		5. Available time, 2008 X A		= 56224 (hrs)	E
		6. Productive time, E - D		= 49192 (hrs)	F
		7. Leave factor, D ÷ F + 1.00		= 1.14	G
		8. % leave rate = D ÷ E X 100		= 13 %	

AMS RECAP:

AMS CODE	FTP	TPT	ALLOC STR OFF	ALLOC STR ENL	ALLOC STR TOT	RECOMD BY COMD FTP	RECOMD BY COMD TPT	RECOMD BY COMD OFF	RECOMD BY COMD ENL	RECOMD BY COMD TOT

* U.S. GPO: 1973—540-841/8843

Figure T-7 Continued—(p. 24 of 35).

MANPOWER SURVEY REPORT -SCHEDULE X - MANPOWER AND WORKLOAD DATA

For use of this form, see AR 570-4; the proponent agency is the Office of the Assistant Chief of Staff for Force Development.

REPORTS CONTROL SYMBOL CSFOR-76

MAJOR STAFF ELEMENT	DIVISION	BRANCH	SECTION OR UNIT	SHEET NO.	LINE NO.
Dir for Admin	Security	Security Br No. 2		8	6

DESCRIPTION OF WORK PERFORMED

Develops, implements, and enforces traffic regulations and maintains security of installation.

YARDSTICK CODE: 570-566-34.3

WORK UNIT: Posts & Patrols

SECTION A - SUMMARY OF MANPOWER

	OFF a	WO b	ENL c	US CIV d	NON-US CIV e	TOTAL MAN-POWER SUBJ TO ALLOC f	OTHER MANPOWER US g	OTHER MANPOWER NON-US h	TOTALS i
1. ALLOCATION				30		30			30
2. ACTUAL STRENGTH				27		27			27
3. RECM BY CO				32		32			32
4. RECM BY SURVEY TEAM				31		31			31

YARDSTICK ALLOWANCE COMPUTATION

SECTION B - PERFORMANCE DATA

YEAR AND MONTH 19 77 -78	MANPOWER: AVG STR b	MANPOWER: TOTAL MAN-HOURS WORKED c	MANPOWER: HRS OP IN MO d	MANPOWER: EQUIV MAN-MONTHS (c ÷ d) e	WORKLOAD: NO. OF WORK UNITS f	WORKLOAD: W/L PER PERSON (f ÷ e) g
SEP	28	4181	160	26.1		
OCT	27	4333	168	25.8		
NOV	28	4324	160	27.0		
DEC	28	4411	168	26.2		
JAN	31	5490	176	31.2		
FEB	32	4987	152	32.8		
MAR	32	5368	168	32.0		
APR	29	5305	176	30.1		
MAY	31	5372	168	32.0		
JUN	29	4619	168	27.5		
JUL	28	4606	176	26.2		
AUG	27	4578	168	27.2		
1. WORKLOAD USED AS BASIS OF APPRAISAL						
2. AVERAGE PRODUCTIVITY						

3. MANPOWER ALLOWANCE

SURVEY WORKLOAD (1) ( ) / AVG PRODUCTIVITY (2) ( ) = ______ × 1.11 = ______

SECTION C - MANPOWER

ALLOC STR a	RANK OR GRADE b	ACTUAL STR c	RANK OR GRADE d	JOB TITLE e
1	GS-08	1		Guard Supy
1	GS-07	1		Guard Supy
12	GS-05	11		Guard
13	GS-04	14		Guard
(27)		(27)		
TEMP	SPACES	SUBJ TO	AUTH	
3	GS-04			Guard
(3)				
SEE SURVEY TEAM REMARKS SHEET 8, LINE 4a FOR RATIONALE LEADING				
TO RECOMMENDED STAFFING.				
30		27		TOTAL

AMS CODE: 36AHG

TDA PARA: 017B

DA FORM 140-4, 1 NOV 73   PREVIOUS EDITIONS OF THIS FORM ARE OBSOLETE.

Figure T-7 Continued—Workload data No. 4 (p. 25 of 35).

SECTION D - SPECIFIC REMARKS

COMMANDER

COMMANDER'S RECOMMENDED STAFFING

DIME'S CATEGORY	COVERABLE	COVERED
I		
II		
III	32	27
IV		

☆ U.S. GPO: 1973—540-841/8543

Figure T-7 Continued—(p. 26 of 35).

SECTION D - SPECIFIC REMARKS

COMMANDER

Summary of actual manhours, leave computation and recap of authorized and recommended spaces by AMS codes follows:

ACTUAL MANHOURS (Survey Period)	
Borrowed	
Loaned	
Overtime	6349
Ann Lv	4831
Sick Lv	2346
Other Lv	137
Civ TDY	
Mil Lv	

LEAVE FACTOR

1. Actual Strength, Aug 77 (civ + mil) = 27 (pers) A
2. Sick leave, 62 X A = 1674 (hrs) B
3. Annual Leave
   - CAT 8 (incl mil) 208 X 17 = 3536 (hrs)
   - CAT 6 160 X 9 = 1440 (hrs)
   - CAT 4 104 X 1 = 104 (hrs)
   - SUM OF 3 = 5080 (hrs) C
4. Nonproductive leave time B + C = 6754 (hrs) D
5. Available time, 2008 X A = 54216 (hrs) E
6. Productive time, E - D = 47462 (hrs) F
7. Leave factor, D ÷ F + 1.00 = 1.14 G
8. % leave rate = D ÷ E X 100 = 12 %

AMS RECAP:

AMS CODE	FTP	TPT	ALLOC STR OFF	ALLOC STR ENL	TOT	FTP	TPT	RECOMD BY COMD OFF	RECOMD BY COMD ENL	TOT

U.S. GPO: 1973—540-841/8543

Figure T-7 Continued—(p. 27 of 35).

MANPOWER SURVEY REPORT -SCHEDULE X - MANPOWER AND WORKLOAD DATA

For use of this form, see AR 570-4; the proponent agency is the Office of the Assistant Chief of Staff for Force Development.

REPORTS CONTROL SYMBOL CSFOR-76

MAJOR STAFF ELEMENT	DIVISION	BRANCH	SECTION OR UNIT	SHEET NO.	LINE NO.
Dir for Admin	Security	Security Br No. 3		8	7

DESCRIPTION OF WORK PERFORMED

Develops, implements, and enforces traffic regulations and maintains securiry of the installation.

YARDSTICK CODE: 570-566-34.3

WORK UNIT: Posts & Patrols

SECTION A - SUMMARY OF MANPOWER

	OFF a	WO b	ENL c	US CIV d	NON-US CIV e	TOTAL MAN-POWER SUBJ TO ALLOC f	OTHER MANPOWER US g	OTHER MANPOWER NON-US h	TOTALS i
1. ALLOCATION				30		30			30
2. ACTUAL STRENGTH				27		27			27
3. RECM BY CO				32		32			32
4. RECM BY SURVEY TEAM				31		31			31

YARDSTICK ALLOWANCE COMPUTATION

SECTION B - PERFORMANCE DATA

YEAR AND MONTH 19 76 / 77	MANPOWER: AVG STR b	MANPOWER: TOTAL MAN-HOURS WORKED c	MANPOWER: HRS OP IN MO d	MANPOWER: EQUIV MAN-MONTHS (c ÷ d) e	WORKLOAD: NO. OF WORK UNITS f	WORKLOAD: W/L PER PERSON (f ÷ e) g
SEP	28	4490	160	28.1		
OCT	28	4365	168	26.0		
NOV	29	4522	160	28.3		
DEC	29	4742	168	28.2		
JAN	29	5157	176	29.3		
FEB	31	4787	152	31.5		
MAR	30	4913	168	29.2		
APR	29	4842	176	27.5		
MAY	29	4884	168	29.1		
JUN	27	4330	168	25.8		
JUL	27	4681	176	26.6		
AUG	27	4215	168	25.1		

1. WORKLOAD USED AS BASIS OF APPRAISAL

2. AVERAGE PRODUCTIVITY

3. MANPOWER ALLOWANCE

SURVEY WORKLOAD (1) ( ) / AVG PRODUCTIVITY (2) ( ) = ____ × 1.11 = ____

SECTION C - MANPOWER

ALLOC STR a	RANK OR GRADE b	ACTUAL STR c	RANK OR GRADE d	JOB TITLE e
1	GS-08	1		Guard Supy
1	GS-07	1		Guard Supy
12	GS-05	10		Guard
13	GS-04	15		Guard
(27)		(27)		
TEMP SPACES SUBJ TO AUTH				
3	GS-04			Guard
(3)				
SEE SURVEY TEAM REMARKS, SHEET 8, LINE 4a FOR RATIONALE				
LEADING TO RECOMMENDED STAFFING.				
30		27		TOTAL

AMS CODE: 36AHG

TDA PARA: 017C

DA FORM 1 NOV 73 140-4 PREVIOUS EDITIONS OF THIS FORM ARE OBSOLETE.

Figure T-7 Continued—Workload data No. 5 (p. 28 of 35).

SECTION D - SPECIFIC REMARKS

COMMANDER

COMMANDER'S RECOMMENDED STAFFING

DIME'S CATEGORY	COVERABLE	COVERED
I		
II		
III	32	27
IV		

☆ U.S. GPO: 1973—540-841/8843

Figure T-7 Continued—(p. 29 of 35).

SECTION D - SPECIFIC REMARKS

COMMANDER

Summary of actual manhours, leave computation and recap of authorized and recommended spaces by AMS codes follows:

ACTUAL MANHOURS (Survey Period)	
Borrowed	
Loaned	
Overtime	6025
Ann Lv	4339
Sick Lv	2224
Other Lv	816
Civ TDY	
Mil Lv	

LEAVE FACTOR

1.	Actual Strength, Aug 77 (civ + mil)		= 27 (pers)	A
2.	Sick leave, 62 X A		= 1674 (hrs)	B
3.	Annual Leave			
	CAT 8 (incl mil)	208 X 16 = 3328 (hrs)		
	CAT 6	160 X 11 = 1760 (hrs)		
	CAT 4	104 X = ____ (hrs)		
	SUM OF 3		= 5088 (hrs)	C
4.	Nonproductive leave time B + C		= 6762 (hrs)	D
5.	Available time, 2008 X A		= 54216 (hrs)	E
6.	Productive time, E - D		= 47454 (hrs)	F
7.	Leave factor, D ÷ F + 1.00		= 1.14	G
8.	% leave rate = D ÷ E X 100		= 12 %	

AMS RECAP:

AMS CODE	ALLOC STR FTP	ALLOC STR TPT	ALLOC STR OFF	ALLOC STR ENL	ALLOC STR TOT	RECOMD BY COMD FTP	RECOMD BY COMD TPT	RECOMD BY COMD OFF	RECOMD BY COMD ENL	RECOMD BY COMD TOT

☆ U.S. GPO: 1973—540-841/8543

Figure T-7 Continued—(p. 30 of 35).

MANPOWER SURVEY REPORT - SCHEDULE X - MANPOWER AND WORKLOAD DATA

For use of this form, see AR 570-4; the proponent agency is the Office of the Assistant Chief of Staff for Force Development.

REPORTS CONTROL SYMBOL CSFOR-76

MAJOR STAFF ELEMENT	DIVISION	BRANCH	SECTION OR UNIT	SHEET NO.	LINE NO.
Dir for Admin	Security	Intelligence & Investigations		8	8

DESCRIPTION OF WORK PERFORMED Conducts investigations concerning incidents perpetrated by post or installation employees which occur on installation premises, at assigned off-post premises, or at dependents' housing areas. Implements crime prevention program. Recovers lost or stolen military or civilian property. Maintains continuing surveillance for purposes of uncovering acts of fraud, malfeasance and misfeasance, and locates areas susceptible to pilferage. Conducts preemployment character investigations and maintains personnel

YARDSTICK CODE

WORK UNIT 566-34.2

SECTION A - SUMMARY OF MANPOWER

	OFF a	WO b	ENL c	US CIV d	NON-US CIV e	TOTAL MAN-POWER SUBJ TO ALLOC f	OTHER MANPOWER US g	OTHER MANPOWER NON-US h	TOTALS i
1. ALLOCATION									
2. ACTUAL STRENGTH									
3. RECM BY CO									
4. RECM BY SURVEY TEAM				7		7			7

YARDSTICK ALLOWANCE COMPUTATION

L. A.

SECTION B - PERFORMANCE DATA

YEAR AND MONTH 1977 78	MANPOWER: AVG STR b	MANPOWER: TOTAL MAN-HOURS WORKED c	MANPOWER: HRS OP IN MO d	MANPOWER: EQUIV MAN-MONTHS (c ÷ d) e	WORKLOAD: NO. OF WORK UNITS f	WORKLOAD: W/L PER PERSON (f ÷ e) g
SEP			160			
OCT			168			
NOV			160			
DEC			168			
JAN			176			
FEB			152			
MAR			168			
APR			176			
MAY			168			
JUN			168			
JUL			176			
AUG			168			
1. WORKLOAD USED AS BASIS OF APPRAISAL						
2. AVERAGE PRODUCTIVITY						

3. MANPOWER ALLOWANCE

SURVEY WORKLOAD (1) ( ) / AVG PRODUCTIVITY (2) ( ) = ____ × 1.11 = ______

SECTION C - MANPOWER

ALLOC STR a	RANK OR GRADE b	ACTUAL STR c	RANK OR GRADE d	JOB TITLE e
			GS-11	Security Officer
			GS-09	Investigator
			GS-09	Physical Security Spec
			GS-05	Pers Sec Clerk
			GS-04	Inves Student Trainee
			GS-03	Clerk General
			GS-03	Clerk Typing
				TOTAL

AMS CODE:

TDA PARA:

DA FORM 1 NOV 73 140-4 PREVIOUS EDITIONS OF THIS FORM ARE OBSOLETE.

Figure T-7 Continued—Workload data No. 6 (p. 31 of 35).

SECTION D - SPECIFIC REMARKS

COMMANDER

COMMANDER'S RECOMMENDED STAFFING

DIME'S CATEGORY	COVERABLE	COVERED
I		
II		
III		
IV		

☆ U.S. GPO: 1973—940-841/8843

Figure T-7 Continued—(p. 32 of 35).

SHEET NO. 8 | LINE NO. 8-1

DESCRIPTION OF WORK PERFORMED.

identification system including fabrication and issue of personnel identification badges, and maintain privately owned vehicle registration system. Plans, installs and maintains the installation key and lock system and maintains master key set. Sets and adjusts security containers. Provides visitor control and arranges for escort for visitors. Registers privately owned firearms and pets of personnel residing on the installation.

Figure T-7 Continued—Continuation sheet (p. 33 of 35).

MANPOWER SURVEY REPORT - REMARKS For use of this form, see AR 570-4; the proponent agency is DCSPER.	1. SHEET NO.	2. LINE NO.	REPORTS CONTROL SYMBOL
	8	8-2	CSFOR-76

3. CHECK APPLICABLE BLOCK. ☐ SURVEY TEAM GENERAL REMARKS (complete item 4, only, and file after Commander's General Remarks.)
☐ COMMANDER GENERAL REMARKS (complete item 4, only, and file after Coversheet, DA Form 140.)
☒ SURVEY TEAM SPECIFIC REMARKS (If this block is checked, complete items 1, 2, and 4 and file with Schedule X.)

4. REMARKS: (If more space is required, continue on plain paper 10½" x 8".)

a. The survey team recommends 7 civilian spaces for this activity.

b. Recommendation is based on governing survey rationale presented in Survey Team General Remarks.

c. Other considerations included:

(1) The survey team recommends establishment of an Intelligence and Investigations Branch in the Security Office and realinement of functions previously performed in the Office of the Chief.

(2) The survey team recommends the following minimum essential staffing to perform the missions and functions of the Intelligence and Investigation activity.

(3) Workload projections and priorities recognized by the survey team are as follows:

(a) Conducts investigations concerning incidents perpetrated by post employees which occur on post premises, at assigned off-post premises, or at dependents' housing areas. Implements crime prevention program. Recovers lost or stolen military or civilian property. Maintains continuing surveillance for purposes of uncovering acts of fraud, malfeasance and misfeasance. Locates areas susceptible to pilferage.
1.5 Manyear

(b) Lock and Key Control: Performs the security key and lock system and 17 subsystems required to supplement other security measures utilized in controlling access to security areas to include control, issue and rotation of keys/locks. (Approximately 1564 Locks/Keys). .5 Manyear

(c) Conducts pre-employment character investigations and maintains personnel identification system including:

Annual private-owned vehicle inspection. (AR 190-5-1, 12 Nov 76)
Privately-owned vehicle registration.
Fabrication and issue of personnel identification badges.
Special passes.
Provides visitor control.
Arranges for escort for visitors.
Registers privately-owned firearms and pets of personnel residing on installation. 3 Manyears

FOR EXAMPLES AND INSTRUCTIONS, SEE APPENDIX B, DA PAMPHLET 570-4.

DA FORM 1 DEC 73 140-1 PREVIOUS EDITIONS OF THIS FORM ARE OBSOLETE. ★ U.S. GPO: 1975—580-842/8429

Figure T-7 Continued—Remarks (p. 34 of 35).

MANPOWER SURVEY REPORT - REMARKS

For use of this form, see AR 570-4; the proponent agency is DCSPER.

1. SHEET NO.	2. LINE NO.	REPORTS CONTROL SYMBOL
8	8-3	CSFOR-76

3. CHECK APPLICABLE BLOCK. ☐ SURVEY TEAM GENERAL REMARKS *(complete item 4, only, and file after Commander's General Remarks.)*

☐ COMMANDER GENERAL REMARKS *(complete item 4, only, and file after Coversheet, DA Form 140.)*

X SURVEY TEAM SPECIFIC REMARKS *(If this block is checked, complete items 1, 2, and 4 and file with Schedule X.)*

4. REMARKS: *(If more space is required, continue on plain paper 10½" x 8".)*

(d) The survey team recognizes the space for investigative student trainee as part of the post massive training program. This space is considered nonproductive as the student reports for duty during the summer months and during Christmas holidays and semester breaks. The survey team also recognizes the requirement for clerk typist for clerical and typing functions.

d. The Security Officer (Sheet 8, Line 4) will serve in a dual capacity, i.e., Chief of the Intelligence and Investigations Branch.

FOR EXAMPLES AND INSTRUCTIONS, SEE APPENDIX B, DA PAMPHLET 570-4.

DA FORM 140-1, 1 DEC 73 — PREVIOUS EDITIONS OF THIS FORM ARE OBSOLETE. ★ U.S. GPO: 1975—580-842/8429

Figure T-7 Continued—(p. 35 of 35).

Appendix U

Convoys, Trains, And Pipelines

Military police responsibility for physical security of convoys, trains, and pipelines can vary greatly in combat and peacetime. And it can vary greatly in degree within these two situations. Convoy security can bean MP unit's responsibility only while the convoy passes through the unit's area; or it can be the unit's responsibility from the point of origin to the point of delivery. During railroad security, MPs work closely with transportation railway service personnel. Pipelines present a very difficult security task. These highly vulnerable and volatile arteries are critical to our peacetime and war effort and must be protected from end to end. This appendix offers details on how best to meet the physical security requirements for each of these tasks.

153-846 O - 94 - 21

U-1 Definition

a. A **convoy** is a march column of vehicles moving over the same route for a single movement under the centralized control of a single commander. This column commander is designated by the major commander controlling the movements control center. He may also be designated by the commander of the organization initiating the convoy.

b. Size. A convoy may be one group of vehicles, or it may be broken down into subdivisions, each under control of a subordinate commander. A **serial** is the major subdivision; it may be broken further into **march units.** In some recorded instances, the serial has been eliminated, as in a convoy of 60 vehicles organized into four 15-vehicle march units. Organization depends on many factors. Some of these are road conditions, travel distance, terrain, weather, enemy activity, and the training and experience of all personnel. Normally, a column of 20 or less vehicles is not broken down, since they can all be controlled by one commander. If more than 20 vehicles are involved, the convoy should be broken down because of the difficulty of control in terms of column length.

U-2 Operation

Convoy escort and security is an operation in which military police are **detailed to provide security and movement** to a specific group of vehicles. MPs may be called onto help numerous kinds of convoys, to include the following.

- Resupply operations.
- Special ammunition or sensitive material movements.
- Escort of designated commanders and other VIPs.
- Assistance to combat arms units during difficult movements, such as passage of lines or river crossings.

The **area commander** (theater Army, corps, division), through HTH, **allocates MP resources** to convoy security missions. A primary consideration is whether or not the convoy is able to provide its own security. For example, an infantry battalion has the organic weapons to provide its own security; a light truck transportation battalion may not. The specific tactical situation is also a concern, particularly when rear area protection is a factor. Military convoy operations in CONUS are discussed in detail in TM 55-312. Military convoy operations for stability operations are covered in TM 55-311.

U-3 MP Commitment

Military police are committed for convoys in one of two ways—are-oriented or functional-oriented support.

a. In **area-oriented support,** the MP unit provides MP support within a geographical area. The unit would escort a convoy from the time it enters this area until it leaves the area.

b. In **functional-oriented support,** the MP unit performs a specific task. This unit would escort a convoy from start to finish, regardless of areas passed through.

U-4 Controls

Convoy movements are usually controlled by two methods—organizational and area control.

a. Organizational control is the responsibility of the commander of the organization or unit using the road. In this case, the commander is concerned with enforcing observance by his drivers of the rules of the road. These rules include traffic laws and regulations, speeds, vehicle distance, routing, time schedules, discipline en route and at halts and local security measures. Organizational control is the rule under peacetime conditions in CONUS and in secure oversea areas. Military police become involved in such functions for traffic control at critical points, escorts through congested areas, and security of critical or sensitive cargo.

b. Area control is the responsibility of the commander having area jurisdiction. This is the more common type of control exercised in an active theater of operations. It is superimposed on organizational control. It is employed only to the extent necessary to assure orderly and effective movement of vehicles over the highway system. It is exercised by a central office, such as a movements control center in the transportation command, or a division transportation office (for a movement entirely within the division area of responsibility).

U-5 Function, Intelligence Placement, and Command

a. Function. Escort and security elements accompany a column or convoy, **assist the convoy's movement,** and protect **it from interference** from any source. Convoy escort and security elements are placed in direct support of the convoy. The security elements may consist of military police, civilian police, or other personnel assigned to accompany the column through congested areas or areas of possible traffic conflict of armed guards, ground troops, or armed aircraft to protect the movement from sabotage, pilferage, guerrilla activity, or enemy action; or any combination of the foregoing. Military police performing as escorts or security elements will normally be assigned only to high priority missions.

b. Military intelligence. Prior to the movement of convoys, coordination should be effected with the military intelligence unit providing counterintelligence coverage through the area to be traveled. This coordination may provide additional security coverage. It may reveal information on potential guerrilla, terrorist, or sabotage activities along the intended route.

c. Placement. Convoy escort and security elements perform their functions on mission-type commitments. They comply with pertinent command directives and the en route requirements of the convoy commander. The location of these elements within the convoy is determined by locally established policies and procedures; the enemy, weather, and terrain situation; current area intelligence; troops available; availability of armored or hardened vehicles; and experience of the convoy commander and escort and security personnel.

d. Security Element Control. In some instances, particularly with small convoys, the convoy commander may also be the commander of the escort and security force. In

other situations, someone other than the commander may be in control, depending on policies established by the responsible commander. In large convoys, which may include 75 to 150 vehicles, the convoy commander is usually a Transportation Corps officer. He exercises control over the escort and security element through the element commander. In either case, the escort and security commander normally plans, coordinates, and integrates all matters pertaining to security of the convoy, to include noise and light discipline requirements; front, flank, and rear security during movement and halts; air cover; fire support; communications with supporting units and higher headquarters; and interrogation of local civilians along the route to develop current intelligence information concerning road conditions and possible guerrilla or enemy activities.

U-6 Convoy SOP

a. Planning. The degree of success or failure of military convoys is in direct proportion to the planning that precedes its execution. A comprehensive standing operating procedure (SOP) facilitates planning. It provides guidance in various situations in the absence of orders. The SOP must not standardize any procedures into patterns that would indicate to the enemy the anticipated or predictable action of convoy personnel. When routes are established and alternates do not exist, it is advisable to operate on these routes on an irregular schedule. This decreases the convoy's vulnerability to deliberate ambushes. Departure points, halts, and refueling points should be varied when possible to help keep ambush forces off balance.

b. Content. SOPs at company level should conform with SOPs prepared by the next higher headquarters. The local situation and type of operation will influence the scope of each SOP. The following minimum actions must be covered:

(1) Approval authority for convoy movements.

(2) Duties of convoy commanders and control personnel.

(3) Convoy organization and communication.

(4) Weapons and ammunition to be carried.

(5) "Hardening" of vehicles (adding armorplating).

(6) Protective equipment worn by personnel.

(7) Preparation of convoy vehicles, such as detailed instructions regarding tarpaulins, tailgates, and windshields.

(8) Counterambush action.

(9) Security measures.

(10) Maintenance and recovery of disabled vehicles.

(11) Refueling and rest halts.

(12) Safety measures.

c. Training in convoy operations and counteambush measures should conform as closely as possible to the SOP. This will help insure that personnel are adequately trained to cope with probable situations.

d. Military police assigned to convoy escort duties must be familiar with the SOP of the convoy personnel. The MPs must insure their own SOP is compatible with that of the escorted unit. Exchange of information concerning training and matters of mutual interest aids successful completion of the mission.

e. Convoy air support. Consideration should be given to the use of air cover for security of the convoy. It also maybe used as

a reaction force if the convoy is ambushed. The air element of the convoy security force might consist of one aircraft or more.

U-7 Multi-unit Convoys.

a. Convoys frequently are composed of vehicles and personnel from more than one unit. In some circumstances vehicles are a part of units only remotely related to the command responsible for the convoy organization. This situation may occur when various units must move personnel or equipment over lines of communications. These units may wish to take advantage of the security normally provided a large convoy. Additions of this type are referred to as add-ons. The arrival of unscheduled units at the assembly area with the intention of joining the convoy may disrupt the organization plan. This can be prevented by units making advance notice of their intentions. The notices should arrive at the responsible headquarters 24 hours before convoy departure time. This allows officers to make necessary adjustments for integration of additional vehicles into the march elements.

b. Local nationals who gather around vehicles in the assembly area or during scheduled or unscheduled halts are a potential source of sabotage and pilferage. **Unauthorized personnel should be kept out of the assembly area.** They should be kept at a safe distance from halted vehicles. Convoy and escort personnel should be alert for any hostile act. They should wear protective equipment and keep their weapons in hand.

U-8 Vehicle Preparation

a. Maintenance. Emphasis must be placed on the importance of preparing vehicles for a convoy operation. When a truck has a mechanical failure in an area infested by insurgents, the truck and its cargo may have to be destroyed. Even when repairs can be made on the spot or the truck taken in tow,

Convoy Vehicle Checklist

- ☐ Air hose couplings
- ☐ Oil and lubrication levels
- ☐ Cooling system
- ☐ Tires
- ☐ Brakes
- ☐ Battery.

Supervisory personnel should check for:

- ☐ Availability of additional fuel, water, and lubricants.
- ☐ Windshield in prescribed position.
- ☐ Tarpaulin and end curtains when required.
- ☐ Condition of sandbags in the driver's compartment and in cargo bed when required.
- ☐ Weapons mounted on vehicles must be inspected.

some elements of the column will be delayed. This increases their exposure to ambush, snipers, or terrorist attacks.

b. Unit commander's responsibilities. The commander of the unit furnishing vehicles for a convoy and for a convoy security escort is responsible for their condition. Before dispatching vehicles to the convoy assembly points, each vehicle should be thoroughly inspected by qualified maintenance personnel. (See checklist on page 469.)

c. Assembly area inspection teams. Trucks scheduled for the convoy normally arrive at the assembly area during the night prior to departure time. To insure all vehicles are in satisfactory mechanical condition, the convoy commander may appoint a night maintenance inspection team to inspect vehicles on arrival. Minor deficiencies must be corrected on the spot. Vehicles with major deficiencies must be returned to the parent unit and replaced with satisfactory ones. Under no circumstances will a mechanically defective vehicle be allowed to depart with the convoy. **A comparable procedure should be followed with military police security escort vehicles.**

d. Windshields. Unless prescribed by higher headquarters, the convoy commander should consider the following when deciding whether to have windshields removed, lowered, or left in place. Windshields left in place provide protection against heavy dust and driving rain. They also serve as a connecting point for chicken wire that may be secured to each window to protect against incoming grenades. They provide protection from wire stretched across the road to decapitate personnel. However, windshields should be removed when they interfere with the use of weapons, and during blackout operations. To prevent windshields from breaking because of shock and vibration when lowered, a piece of plywood or similar material covered with sandbags should be placed between the windshield and the hood.

e. Hardening vehicles. The floors of troop-carrying vehicles should be covered with at least a double interlocking layer of sandbags. Cab floors of all vehicles should be sandbagged with a double layer under the driver's seat. As an additional precaution, a heavy rubber or fiber mat is recommended over the sandbags to reduce danger from fragments such as stones, sand, metal parts of the vehicle, and shrapnel. The life of sandbags is prolonged when the sandbags are covered by a mat. Sandbags also may be placed on the gas tank, fenders, and hood. Armorplating may be installed on general purpose vehicles when authorized by the responsible commander. Fuel tanks can be hardened by inserting steel plates between the fuel tanks and hanger straps.

f. Tarpaulins and cab tops.

(1) In some areas the use of tarpaulins, canvas truck tops, and cab tops is decided by the responsible area commander. In other areas, it may be left to the discretion of the responsible convoy commander. When the decision is made by the convoy commander, he should weigh the disadvantages against the advantages. (It can be assumed that when cargo will be damaged by prevailing weather conditions, it will be covered.)

(2) The **principal advantage** in covering a shipment is that it makes it more difficult for an ambush force to identify critical cargo such as ammunition and POL products-always a preferred target.

(3) The **main disadvantage** of using truck top or tarpaulins is that they have to be removed for loading and unloading operations; thus reducing the operating time of the truck. In some instances, a truck top interferes with the driver's vision to the rear and with the gunner firing to the rear—a distinct disadvantage.

(4) By leaving the cab top on **POL loaded vehicles,** some protection is afforded the driver if the cargo tank ruptures and the

contents are ignited. Tankers of 1,200-gallon capacity can be effectively disguised by rigging bows and canvas over the cargo tank. Except at very close range, this gives the appearance of a general purpose 2½-ton truck.

g. Additional precautions. Loaded vehicles in the assembly area present a profitable target to the enemy. To prevent sabotage, the area should be secure against ene my infiltration. When vehicles are equipped with gas cap locking devices, these should be locked. An adequate guard force should be on duty at all times.

U-9 Staff Actions

a. Planning a convoy operation requires high quality, aggressive staff action on the part of the truck unit staff. The officer designated as convoy commander has only a limited period to reconnoiter the route. He must give instructions to subordinate element commanders and other supervisory personnel, and achieve final coordination with the security force commander. These duties cannot be neglected for functions that are a truck unit staff responsibility.

b. Units through whose tactical areas of responsibility the convoy is to be moved must be contacted. This is to determine what restrictions and requirements are placed on convoys in each area and what convoy support can be furnished This support could include the following:

Security forces
Escort vehicles
Fire support
Vehicle recovery and repair
Engineer road repair
Medical support.

Any special problems that may interfere with the convoy must be reconciled. After this information has been collected, the staff can complete planning for fire support, road outposting and clearing, escort forces, and engineer support. Based on this information, detailed instructions go to the convoy commander and affected units in an operations order. The operations order does not eliminate the requirement for a briefing. This is usually conducted by members of the battalion staff.

U-10 Convoy Commander

a. Briefing. An officer or NCO appointed as convoy commander should contact the unit S3 officer and determine when he can be briefed for the operation. The briefing should cover all topics mentioned in paragraph U-9 and any others affecting the convoy. The convoy commander should ask questions on any facet not covered or not clear. When the responsible staff officer cannot answer the question, he should get the answer, while the convoy commander is present, if possible. Before leaving the briefing, the convoy commander should bring his maps up to date.

b. Route reconnaissance. If a choice of routes is possible, the decision of which route to be used will depend on these factors:

- Time.
- Distance.
- Current and expected enemy activity.
- Availability of security forces.
- Availability of fire support along the selected route.
- Trafficability of the roadbed and any bridges.
- Other critical factors.

In many instances the route will be prescribed by higher headquarters. In this case a map reconnaissance will enable the convoy commander and the unit staff to select tentative checkpoints or confirm those already

established. This reconnaissance should ascertain all units whose tactical areas of responsibility they will pass through. It should also identify potential trouble areas and ambush sites.

After the map reconnaissance is completed and the route selected, the convoy commander should conduct either a ground or aerial reconnaissance of the road. If aerial reconnaissance is made, it should be conducted, whenever possible, several times prior to the date scheduled for the convoy. As many subordinate convoy leaders as possible should be included in these reconnaissance flights. This enhances the convoy commander's briefing of the convoy leaders on the route and its potential trouble areas.

Military police should be able to conduct a hasty reconnaissance of the route to be used by the convoy. At least a map reconnaissance is necessary. All sources of information should be consulted, especially the engineers and highway traffic headquarters. Aircraft should be used if possible. Classification of the route is important.

The following administrative color codes are used to classify roads. (Designations are made on the basis of intelligence available at the time. The designation can be incorrect.)

- **Green-generally free from enemy** activity and may be used unarmed.

- **Yellow-risk of enemy activity.** All military personnel should be armed and each vehicle should carry at least two persons.

- **Red-in the combat zone** and may require offensive or defensive action by combat troops in the field.

c. Fire support and coordination. The convoy commander should not rely on his knowledge of the battery's call sign and frequency in lieu of direct coordination. An artillery unit sets up priorities of fire for the units it supports. A staff officer or the convoy commander must coordinate to obtain a priority for the convoy. If a request for a fire mission is received from an unknown observer, time could be lost in establishing his identity. Information furnished the artillery unit should include the convoy's start and release points, time schedule, checkpoints, and size. Call signs, frequencies, and other signal operating instructions (SOI) should be exchanged. Information received from the area security officer or obtained by route reconnaissance, regarding critical areas of enemy activity is important. It should be used to plan additional fire along the route. An overlay may be pre pared for the convoy commander's map, showing the reference points and concentrations planned by the artillery. Fire can be called for and adjusted from these points much more quickly and with greater accuracy than if unplanned. Further coordination may include

- Types of ammunition to be fired under various conditions.

- Number of rounds to be fired at a given target.

- Types of targets that warrant fire missions.

Any no fire zones should be designated. If the artillery unit cannot provide support along the entire route, its range limitation should be noted on the map. Actual calls for fire missions and adjustment of fire should also be coordinated and rehearsed, even though these calls are standard throughout the Army. The convoy commander may coordinate fire on the assumption that the artillery officer is the authority on fire support. He is capable of planning available artillery resources to the convoy's best advantage.

Another element of fire support that should be planned is the use of gun ships and airborne rocket artillery (ARA). Through coordination, these guns ships and ARA can be either on alert status or overhead while the convoy is en route. In either situation, their radio frequencies must be known to convoy radio operators and control personnel. A means of marking the target should be established. to obtain the full benefit of these weapons systems. All communications and con-

trol personnel should be trained in calling for and adjusting artillery fire.

d. Convoy organization. After being briefed by members of the unit staff, the convoy commander should have sufficient information to enable him to prepare his convoy organization plan. Local conditions will dictate the details of the plan; however, the following should be considered under most circumstances:

(1) Deployment of vehicles loaded with critical cargo. The convoy commander should give special consideration to the placement of vehicles loaded with ammunition and POL supplies. The grouping of vehicles loaded with critical cargo provides a very profitable and easily identifiable target for the enemy. To avoid giving the ambush force this advantage, POL and ammunition loaded vehicles should be dispersed throughout the march elements comprising the convoy.

Another effective technique which has been used when an ambush is expected, is a 500-meter distance between all vehicles. In many instances, because of the extended vehicle distances, the ambush will not be executed since only a limited number of vehicles will be in the kill zone at any one time. To effectively employ this technique, the convoy commander should be airborne. Overhead surveillance by airborne forward observers and light fire teams must cover the entire length of the column. Oncall artillery, airstrikes, and a ready reaction force must also be available.

(2) Deceptive measures. Deception should be used throughout the convoy, especially on POL and ammunition vehicles. Vehicles may be camouflaged with canvas covered frames or by placing lumber, wire, or other cargo over the primary load.

(3) Control vehicles. Such vehicles, especially the convoy commander's, are priority targets for the ambush force. By taking these vehicles out of action at the onset of an attack, key leaders are eliminated. Consequently, communications with other elements and reaction forces are disrupted. The ambush force can be placed at some disadvantage by avoiding a set pattern in the location of control vehicles. You can create further deception by using a cargo vehicle (2½-ton or 5-ton truck) with radios installed for the command vehicle. When a cargo truck is used, conceal antennas under the truck body. The military police planner decides the best method of escort to use. The types of escorts are described in FM 19-25, Chapter 1, Installation Traffic Control. Considerations are terrain, persons or cargo, volume, length, enemy actions, and resources available to the convoy and MPs. Methods of escorts are:

- ☐ Leading and following
- ☐ Empty truck (or modified)
- ☐ Leapfrog
- ☐ Perimeter.

(4) Maintenance and recovery vehicles. The size of the trail party and the number of recovery vehicles is determined by the size of the convoy and the experience of convoy personnel. Normally, recovery vehicles are assigned to each march element of the convoy. The recovery capability of 5-ton tractors (bobtail) and 2½-ton cargo trucks without trailers and equipped with tow bars should be considered. The availability of these vehicles will leave wreckers free for the recovery of more critically damaged equipment. One tractor truck for every 10 tractor-semitrailer combinations is considered a satisfactory ratio. A radio mounted in the wrecker enables the convoy commander to effectively control vehicle recovery without being physically present. This provides greater flexibility in the march unit communications system.

(5) Armored escort vehicles. The location of escort vehicles in the convoy is dictated by the number available, size of

the convoy, terrain, highway characteristics, enemy situation, availability of reaction forces, and techniques employed by the enemy. One hardened vehicle should be located near the head of the convoy so that fire can be placed on enemy personnel suddenly encountered. The remaining escort vehicles are located where they can provide maximum protection for all convoy elements. Since it is easier for vehicles to move forward than rearward, some escort vehicles must be positioned in the rear of the march element to which they are attached. Under no circumstances should escort vehicles be located where they can be isolated from the convoy by the enemy. They must be able to provide abase of fire for the segment of convoy for which they are responsible.

(6) Unloading. When it will not compromise the security of the convoy, locate trucks requiring the longest unloading time at the head of the march element. This will achieve the fastest turnaround time.

U-11 Command and Control Planning

a. When the operation order is issued, command and control must be completely delineated. This must include:

(1) Chain of command to be followed on the convoy.

(2) Relationship between the convoy commander and the escort commander.

(3) Procedures to be followed in obtaining combat support.

Elements to be on each control frequency should be delineated. This insures proper use of radio nets and complete reporting of essential information. For adequate convoy control there should be a convoy command net. This should include the convoy commander, security force commander, march element commanders, and trail party commander on the net. Each march element should have its control net with the march element commanders, lead and trail escort vehicles, all radio vehicles, and the recovery vehicle in the net.

b. Except in hill country where it may reveal the identity of the command vehicle, control vehicles may be marked with aircraft panel marking. These markers can be numbered with tape for easy identification from the air. Numbers should correspond to the radio call sign of the vehicle.

c. Vehicle distance depends on many variables. Normally it is 50 meters in urban areas with heavy traffic and 100 meters on the open road.

d. Convoy speed depends on the condition of the road, traffic, and on the speed of the slowest vehicle. Airborne command elements using the radio capability can make necessary adjustments to maintain the prescribed vehicle distance and gap between convoy elements. On a long move over rough highways, the speed should not exceed 15 to 20 miles per-hour. Prescribed maximum catchup speed is 25 to 30 miles per hour.

e. Coordination should be made with the local area military police for escorts through populated areas, traffic control at road junctions and other critical points. Road outposting and mine sweeps should be obtained when appropriate.

U-12 Final Convoy Preparation

a. Time required. The convoy must be physically organized. The convoy commander and element commanders must brief personnel. They must also inspect in-

dividual equipment and vehicles. The time for this is influenced by the size of the convoy and the experience of the drivers and control personnel. In planning the convoy preparation schedule, provisions should be made for the lineup of vehicles in the order of march at least 1 hour before start point time.

b. Commander's briefing. The convoy commander holds his briefing after the vehicles have been lined up in the order of march. This briefing should cover at least the following points:

(1) Tactical situation, to include locations of friendly forces, support units, and the enemy situation.

(2) Mission, including types of cargo being transported and the destination.

(3) Execution, to include organization of the convoy, time schedule, routes of march, convoy speed, catchup speed, vehicle distances, and emergency measures to be followed.

(4) Administration and logistics matters, such as control of personnel, billeting and messing of convoy personnel, and refueling and servicing of vehicles.

(5) Command and signal items, to include location of the convoy commander, designation of assistant commander and serial/march unit commander, arm and hand signals, other prearranged signals, and the applicable radio frequencies and call sign.

(6) Safety measures, to include hazards of the route, weather conditions, and defensive driving.

c. Element commander's briefing. After the convoy commander's briefing, personnel return to control of the march element commanders. Here they receive final instructions concerning their elements. Control personnel make final inspections of loads to insure they are properly secured and that vehicles are ready to move.

d. Communications personnel check their equipment and enter the net approximately one half hour before start point time.

e. Guncrews check their weapons and insure they are clear. Rounds are not chambered until a designated geographical marker is reached, or until directed by the convoy commander. When an authorized area is available, guncrews may be directed to test fire their weapons to insure all weapons are operational before departure.

Convoy Commander's Briefing Points

1. Tactical Situation
2. Mission
3. Execution
4. Admin & Logistics
5. Command and Signals
6. Safety

U-13 Rules of Engagement

a. General. The two primary types of engagement likely during convoy movement are **snipers and ambush.** The amount of damage sustained by the convoy when subjected to these attacks is usually in inverse ratio to the amount of training in convoy defense and the adequacy of the briefing convoy personnel have received.

b. Sniper Fire. Extreme caution must be observed when sniper fire is received. We must insure that any return fire does not harm friendly civilians or friendly troops in the area. Especially important is the prevention of indiscriminate firing by convoy personnel without a specific target. The best actions are passive. This should consist of insuring that all personnel wear steel helmets and armored vests at all times. When sniper fire is received, all convoy vehicles should move on through the area without stopping. Escort personnel should:

- Notify the march element commander.
- Give the prescribed signal, usually a red smoke grenade thrown in the direction of the fire.
- Attempt to locate and destroy the sniper by longrange fire if in a free-fire zone.

Fire must not be returned in a no-fire zone. Under order of the convoy commander, additional fire or supporting forces maybe placed in the area to destroy, capture, or drive off the sniper. Convoy personnel should be aware that a heavy volume of fire is frequently employed by the enemy to slow a convoy down just prior to an ambush attack.

c. Ambush Sites. Ambush sites are usually characterized by the following:

(1) Concealment of the ambush force by a screen of foliage, holes dug in the ground, or similar methods.

(2) Good visibility of target area and approaches for the ambush force.

(3) Good field of fire for attacking force.

(4) Good exit route for the attacking force's withdrawal.

(5) Restriction of the attacked element's movements to one flank by natural or man-made obstacles. Natural obstacles include cliffs, steep embankments, swamps, steep grades, sharp curves in the road, narrow trails, streams, and heavily wooded areas. Man-made obstacles usually consist of mines, boobytraps, demolitions, roadblocks, and damaged bridges.

d. Ambush—Road Not Blocked. Extensive road space is occupied by even a platoon size convoy. Because security or lack of available forces may limit the size of the ambushing force, ambush forces are seldom able to contain an entire convoy in a single kill zone. More frequently, a part of a convoy-either head, trail, or a section of the main body is ambushed. The part of a convoy that is in the kill zone and receiving fire must drive out of the ambush if the road to the front is not blocked. Vehicles disabled by enemy fire are left behind. If they are blocking the road, they must be pushed out of the way by following vehicles. Occupants of these vehicles may be picked up by following vehicles.

Armored escort vehicles must not block convoy vehicles by halting in the traveled portion of the road to return enemy fire. Vehicles that have not entered the kill zone must not attempt to run the gauntlet. They should stop, and personnel should dismount and take defensive positions. Since escort vehicles may have left the road to attempt to overrun hostile positions, elements of the convoy should not fire on suspected enemy positions without coordinating with the escort force. Other actions available to convoy personnel for neutralizing the ambush force are:

(1) Call for artillery fire on enemy positions.

Remember:

Vehicles in the kill zone must keep moving!

(2) Call for gun ship fire on enemy positions.

(3) Direct gun trucks and other vehicles mounted with heavy weapons to lay down a heavy volume of fire on the ambush force.

(4) Call for reaction forces.

(5) Direct all nondriving personnel to place a heavy volume of fire on enemy forces as vehicles move out of the kill zone as rapidly as possible.

e. Passive Actions. Actions taken by the convoy commander regarding supporting forces will vary according to the situation. Regardless of his course of action, the element of the convoy caught in the kill zone should clear it as rapidly as possible. A motor transport convoy with a limited escort is seldom able to defeat a hostile force and should not attempt to do so. When part of the convoy is isolated in the kill zone, vehicles that have not entered the ambush area may be required to turn around. They should return to the nearest secured area until supporting forces can clear the ambush. Normally, a transport unit will not deploy to attack a hostile force unless it is necessary to prevent destruction of the convoy elements. However, they will rely on supporting air, artillery, escort, and reaction forces.

f. Ambush—Road Blocked. When an element of a convoy is halted in the kill zone and is unable to proceed due to disabled vehicles, a damaged bridge, or other obstruction, personnel must dismount, take cover, and return a maximum volume of fire on enemy positions. Troops from vehicles that have passed through the ambush area dismount and prepare to attack the flanks of the ambush position. The security force stays behind to protect the vehicles. Personnel in vehicles who have not entered the kill zone follow the same procedure. Before attempting to flank the ambush force, the officer or NCO in charge should insure that his force will not be in the field of artillery fire that may be called in. Reaction forces should be called in as soon as the ambush attack is launched.

When a tactical escort is provided, the officer in command of the escort force takes charge and attempts to neutralize the ambush; otherwise, the senior officer or NCO present takes charge. In an ambush situation, immediate reaction and aggressive leadership are essential in limiting casualties and damage to equipment. The maneuver plan may be altered by the supporting fire plan. Example, if immediate air or artillery is available, personnel are restricted to a specified distance from the road to avoid casualties from friendly fire. In this situation, personnel in the kill zone establish a base of fire. Others take up defensive positions around their vehicles and wait while supporting fire is called in on the enemy positions.

(1) Fire in the kill zone maybe from only one side of the road with a small holding force on the opposite side. To contain the convoy element in the kill zone, mines and boobytraps are frequently placed on the holding force side. Caution must also be taken in assaulting the main ambush force as mines are commonly used to protect its flanks.

(2) When the enemy is dislodged, the road must be cleared. Convoy movement must be resumed as soon as possible. Wounded personnel are evacuated, usually by medical evacuation helicopters. When disabled vehicles cannot be towed, their cargo should be distributed among other vehicles if time permits. When it is not feasible to evacuate vehicles and cargo, they must be destroyed upon orders from the convoy commander. When possible, radios and other critical items are recovered before vehicles are destroyed. Under no circumstances will such items be allowed to fall into enemy hands.

g. Employment of Non-Air Defense Weapons Against Aircraft.

(1) In the absence of orders to the contrary, individual weapons operators will engage attacking aircraft. Engagement of all other hostile aircraft must be on orders issued through the unit chain of command and must be supervised by unit leaders.

(2) A full discussion of this subject area is in FM 44-23, TC 7-1, and TC 23-44.

U-14 Mines and Boobytraps

a. Mines and boobytraps are frequently employed by ambush forces. In fact, a command-detonated mine usually signals an ambush. Mines, either command- or pressure-detonated, vary in size from a few pounds of explosives to several hundred pounds. Some are recovered, unexploded bombs or artillery rounds planted nose up in the road. Mines also are planted along the shoulder of the road for harassment and interdiction. A boobytrap system employed against personnel in vehicles consists of hand grenades attached to tree branches over the road where antennas or other projections from vehicles will snag and detonate the grenades. Claymore mines may be suspended from trees and command detonated when a vehicle passes.

b. The following guidelines have proven effective in decreasing damage by mines in convoy operations:

(1) Track the vehicle in front.

(2) Avoid driving on the shoulder of the road.

(3) Whenever possible do not run over foreign objects, brush or grass in the road.

(4) Avoid fresh earth in the road.

(5) Watch local national traffic and the reaction of people on foot. They frequently give away the location of any mines or boobytraps.

(6) When possible, arrange for the engineers to sweep the road before the convoy is scheduled to move over it.

(7) Heavy vehicles, such as tanks, are useful in exploding small mines when deployed in front of the convoy.

U-15 Halts

a. On long trips it is usually necessary to make one or more scheduled halts for refueling, inspection, and maintenance of equipment, mess, rest, and relief. Locations for halts should be selected before departure of the convoy. They should be situated in a relatively secure area and, when possible, under the surveillance of a security force.

b. The convoy should be halted only at points where there is an unobstructed view of about 200 yards from the head and tail of the column. There should be no restrictions, curves, or grades. Vehicles should be pulled over to the side as far as possible. Drivers should maintain the prescribed vehicle distance. Scheduled halts should not be made in

populated areas or where there is a heavy volume of local traffic, especially on foot. Local civilians should not be allowed to gather around convoy vehicles. All vehicles remain off the road, keeping the traveled portion clear. Guards are required at the head and tail of the column to direct traffic.

U-16 Road and Bridge Damage

Roads or bridges can be damaged, either by natural causes or by the enemy. When alternate routes are not available, engineer support is required to restore the roads to a serviceable condition. One of the benefits of an aerial reconnaissance prior to the convoy's departure is the identification of problem areas along the route. Also, it enhances selection of a bypass or alternate route.

U-17 Vehicle Recovery

a. The assignment of a trained maintenance officer or maintenance sergeant to command the trail party is essential. He must be capable of determining whether a disabled vehicle should be repaired, recovered, or destroyed.

b. The trail party must have security, especially during recovery operations. Trail party vehicles should be hardened and personnel armed with automatic weapons.

c. An effective policy is that the first recovery vehicle to reach a disabled vehicle recovers it unless orders directing other action are received. Normally, a disabled vehicle pulls to the right side of the road to allow those following to continue to move. The shotgunner and any passengers dismount and take up positions from which they can observe possible sniper fire or other enemy action. This protects the driver and vehicle while the driver attempts to repair the vehicle.

(Road shoulders are frequently mined or boobytrapped. Before a driver or crewman dismounts, filled sandbags can be thrown on the ground from the protection of the vehicle, then used as stepping stones. The impact of the sandbags will detonate most pressure type antipersonnel explosive devices near the vehicle.)

When the trail of the march element arrives, the escort vehicle commander notifies the convoy and march element commanders. He then attempts a recovery until the head of the next march element arrives. At this time he returns to his trail escort position.

If the disabled vehicle requires towing, the wrecker or other vehicle to be used, stops 25 to 50 meters in front of the disabled vehicle. The tow bar is then attached to the disabled vehicle. A hasty reconnaissance for mines is conducted in the space between the disabled vehicle and the tow vehicle. Then the tow vehicle is backed into towing position, connected to the disabled vehicle and, if between march elements, moves under escort to the rear of the march element ahead. If in a passing march element, the driver of the tow vehicle waits until the trail of the passing march element arrives. He then takes a position to the rear of the march element. The most important elements in recovery are vehicle security and speed in recovering the disabled vehicle. This recovery keeps the road clear.

The march element and convoy commander must be kept informed of the status of disabled vehicles. If a vehicle is disabled because of a mine, fire, wreck, or enemy weapons, the convoy commander must decide if the vehicle is recoverable. If it appears that recovery is impracticable, he may decide to destroy it in place, provided such action has been authorized by the appropriate commander. This can be performed by the engineers using explosives, by gunfire from the escort force, or by artillery or tactical air fire after the convoy has cleared the area. All personnel should understand that destruction

of equipment is a command decision. Destruction should be employed only to prevent it from falling into the hands of the enemy. Critical parts of the equipment to be destroyed should be recovered if sufficient time is available.

U-18 Release Point

Prior to arrival it is a good policy to contact the receiving units by radio. This notifies them of the expected time of arrival. It enables them to meet the convoy at the release point and guide the vehicles to the proper unloading points. As the vehicles are unloaded, they should be dispersed and after-operation maintenance should be performed. Drivers should be informed where and at what time to assemble for the return trip. Since forward locations present an especially profitable target when a convoy is present, light and noise discipline should be strictly enforced.

U-19 Night Convoys

a. Due to their extreme vulnerability to ambush and sniper fire, night convoys are **not recommended as a routine operation.** However, intermittent night moves that do not set a pattern can be very effective in keeping enemy forces off balance and in maintaining high resupply levels. When employed, night convoys are much smaller than normal day convoys for easier control. Familiar routes should be used.

b. Planning and Coordination. Night convoy moves are planned the same as day moves. Effective coordination between convoy personnel, escort troops, artillery support, and reaction forces becomes more critical as visibility decreases. It is important that all personnel understand the correct use and interpretation of pyrotechnic signals. Night convoys should be made up of vehicles with uniform capabilities. Outsized or overloaded vehicles should be avoided.

c. Speed, Vehicle Distance, and Light Discipline. Whether a convoy moves under blackout conditions or with lights is determined by local conditions. Under blackout conditions, the vehicle distance is closed to approximately 15 to 20 meters. Speed seldom exceeds 5 to 10 miles per hour. When operating with lights, vehicles usually maintain a distance between vehicles of 50 to 100 meters at a speed of 15 to 20 miles per hour.

d. Escorts. Due to control and security difficulties resulting from reduced visibility, it is essential that march elements be organized in easily manageable sizes. They should have an adequate security escort. When possible, additional radios should be provided to insure rapid communication between all elements involved. Gun jeeps, armored cars, helicopters, armored personnel earners, and tanks can be effectively used as escorts and security elements. Tanks with organic searchlights and high firepower can be highly effective deployed throughout the column as security vehicles. In case of an ambush, they may be driven directly into the ambush, employing shock as well as firepower to neutralize the attacking force. As in all ambushes, it is critical that convoy vehicles caught in the kill zone keep moving. Those that have not entered the kill zone must halt until it is safe to proceed.

e. Release Point. Receiving units must have guides available at the release point to expedite the movement of vehicles to their unloading points. Confusion or delay at the release point is an invitation to an ambush with the resulting loss of men, equipment, and supplies.

U-20 After Action Reports

The final action in any convoy escort operation is submission of an after action report. This can be either orally or in writing, depending on occurrences during the trip. The primary purpose of the report is to provide a record of any unusual occurrences. It provides current intelligence and serves as a record of lessons learned.

Railroad Security

Section II

U-21 Vulnerability

a. Railroads are profitable targets for regular and irregular enemy forces. They are particularly vulnerable to guerrilla attack because a train's movement is directly determined by the condition of the rails. Cutting the rails can produce effects comparable to direct attacks—stopping the train or preventing delivery of critical goods.

b. Even when friendly forces dominate the area, railroads present a target for de liberate sabotage or overt attack. These targets are present in CONUS and the the ater of operations. They range from a switch that can be thrown the wrong way to a trestle that can be demolished. The destruction of switches, signals, or trackage may be only harassment, or it may trigger a chain reaction of a larger scope. The destruction of a bridge or a tunnel may disrupt a whole railway system and may require a long time for repair or replacement. Each individual bridge and tunnel must be considered as a separate security problem.

c. Security measures for railroad operations are determined by the. situation and area of operations. General protective measures may include the following:

(1) Route reconnaissance by Army aircraft.

(2) Occupation of critical terrain features along the route prior to and during move ment.

(3) Use of special observation cars that permit surveillance of the entire train.

(4) Placement of the locomotive at the middle of the train to minimize damage to the locomotive in case of sabotage. An alternate method is to place two or three gondola cars, filled with rocks, sand, or other ballast, in front of the engine to absorb the effects of any detonation of mines placed on the railway.

(5) Use of empty and decoy trains to pre cede critical shipments.

(6) Use of escort or scout trains to patrol the right of way.

(7) Use of special armored guard cars.

(8) Placing of mobile maintenance trains in strategic locations along the route or moving with trains.

(9) Consolidation of trains to assure the most economical use of available air cover.

(10) Movement at highest safe speeds through areas where guerrillas or partisans are active.

(11) Placing of security patrols along the length of the line to be traversed.

These measures are discussed in more detail in the following paragraphs.

d. In addition to the train security operations discussed in this section, military police may be tasked to provide security of railway yards.

U-22 Bridge Vulnerability

A railroad bridge, because of the weight it must support, may be rendered unserviceable merely by weakening it. Bridge approaches or abutments are extremely vulnerable to attack. On a single span bridge, the destruction of an abutment is usually sufficient. In this case not only is the bridge wholly or partly demolished, but the destruction of the abutment makes it difficult to obtain a footing for the foundation of a new bridge on the same site. On a multiple span bridge, the demolition of an intermediate pier usually has the same effect as the destruction of an abutment.

U-23 Bridge Security

The security measures appropriate for a bridge are based on its sensitivity. This is determined by the bridge's location, its relation to other structures and alternate routes, and its proximity to populated areas. Usually the most effective security measure is a stationary security force. Mechanical aids may be used to supplement security. Forces should be placed at both ends of the bridge so they can observe its understructure as well as its roadway. The draw-mechanism of drawbridges should be guarded at all times. Guard boats and upstream booms permit inspection of vessels before allowing them to pass under a bridge. The security force should be quartered at a safe distance from the bridge, but near enough for personnel not on duty to be readily available in an emergency. The full length of the bridge should be inspected at irregular intervals. Sentry dogs may be used to supplement personnel.

U-24 Tunnels

The most vulnerable point of a tunnel or tube is the place where it passes through loose or shifting earth, sand, or other unstable material. At such a location, a saboteur may attempt to destroy the lining by placing explosive charges along the crown or upper sides. It may be sufficient to destroy one side of an arch ring in this manner. If this occurs, the pressure of the over-burden may bring down the roof and fill a section of the tunnel. This type of destruction is normally not possible in firm soil or solid rock without the use of large breaching charges. Saboteurs usually avoid this due to the difficulty of placing the charges surreptitiously. However, a similar but not as serious result may be obtained by derailing a train in the tunnel. Ventilating shafts are also vulnerable points.

U-25 Military Police In TRS Security

a. Transportation Railway Service (TRS) personnel are highly trained with one primary mission—to operate and maintain railroads. TRS units are organized especially to fulfill this mission and this mission alone. All TRS personnel have specific jobs in the rail operation. Therefore, security functions beyond the capabilities of TRS units must be handled by those trained and equipped to do the job—the military police.

b. The military police brigade, organic to the area support command in TRANSCOM, provides military police services for the TRS. The brigade has two military police guard battalions, and each battalion has four military police guard companies. One MP guard battalion is assigned to the transportation command for each railway group in the TRS. MP guard companies are assigned on the basis of one per railway battalion.

c. When the TRANSCOM organization does not exist, military police may be detailed for railway security operations from local area MP units.

d. Military police units assigned to the TRS have the specific purpose of providing security for train operations. They may be supplemented by civilian guards; but this practice should be avoided when possible.

e. Train security forces must have all items of equipment and supplies needed for the operation. In addition to their regularly assigned individual weapons (pistols or rifles) and ammunition, special armament may be necessary. They may require bedrolls, rain gear, fire extinguishers, rations, flashlights, lanterns, protective masks, and many similar items. They also must have radios capable of establishing communications with units stationed along or near the railway line. Contact must be established at the earliest opportunity.

f. The NCOIC of the security force should obtain a time schedule for the movement. He should make a map reconnaissance of the route, so he will be able to plan his actions at scheduled stops, at relief points, if any, and to deploy his forces accordingly. He also should plot the locations of military police units and other friendly forces along the route, together with their radio frequencies and call signs. The NCO should establish communication with such units as the train enters their areas of responsibility. This way the units may provide additional support and protection as necessary.

g. The NCOIC also should have an intelligence report covering the route. This provides information as to any sites or locations where sabotage may occur, attacks may be expected, boxcar thievery is on the increase, and similar information.

h. TRS training. Military and civilian security units attached to the TRS should be given a brief training program based on the material presented in this section. This training should familiarize members of these units with basic railway operations, rail terminology, and railway signals. It should also teach them how to coordinate their efforts with those of the train crews for better train protection. All security units should be thoroughly familiar with the requirements of their duties, and know where their duties end and the train crew's begin. The conductor or train commander has the responsibility for the operation and security of his train. He will make all decisions affecting both of these responsibilities. The conductor is the train commander unless a TRS officer is assigned to that train for specific reasons. Close cooperation between train crew members and security forces is imperative.

U-26 Operations Security

a. The primary mission of the train operating crew and the security forces onboard is to get the train to its destination with its freight intact. Normally, a train operating crew consists of four or five people—the engineer, the conductor, a fireman, the senior brakeman, and the brakeman or flalgman-and this crew has control of the train. The number of men in a train security force will depend on:

- Sensitivity of the freight

■ Priority of its need

■ Terrain over which the train will pass.

Security forces may ride in a specific car that requires protection, in the caboose, or in a security car or cars if provided. If only one security car is used, it should be near the center of the train. If more than one is used, spacing should be arranged to provide the best protection for the train. When security forces are assigned to each train, their names are listed on the train dispatcher's roster with the names of the train operating crew. The same security and train crews should, as far as possible, work together on every run. Train crews are either freight or passenger crews, and each type of security force then would need to be trained in only one kind of security Duties differ on passenger and freight trains.

b. The security force on a freight train must keep a constant check on car doors, seals, wires, and locks to detect tampering. They also must be on the alert for cars that may be loaded in a way that would invite pilferage. It is standard railroad practice in making up trains to group the cars according to their respective destinations. However, cars containing easily pilferable freight should be grouped within the train to obtain the most efficient use of security forces. This grouping may be feasible when all cars of the train have the same general destination. When flatcars or gondolas are used for transporting sensitive or easily pilfered freight, the security forces should be placed where they can continuously observe and protect these cars and their freight. If a car is set out on a siding because of a defect, a member of the security force must stay with the car until it is either unloaded or repaired. If more than one car is set out, two or more guards maybe required to protect them.

c. Military police may be assigned to passenger service to help maintain discipline and order. Normally, two men are assigned to a train. They do not interfere with the duties and responsibilities of the train crew. They work with the train conductor on all matters pertaining to the passengers. If they desire to check passes, they do it at the same time as the conductor is checking tickets or the passenger list. Military police assigned to passenger trains should be selected with care be cause their duties involve people rather than inanimate objects of freight. They should possess such personal qualities as tact, poise, and the ability to work harmoniously with others.

U-27 Ground Attack

a. Security of the rail lines, installations, and right-of-way are only part of the job. Trains operating in the threatened area and their freight also must be protected. Military police units attached to the TRS help in accomplishing this task.

b. Underbrush and thick forests should be cleared from the sides of the roadbed to eliminate cover for anyone attempting to interrupt traffic. Railway gondolas carrying mounted machineguns, mortars, and rocket launchers may be manned by military police. Also rail cars loaded with rock and dirt or scrap material may be pushed ahead of the engine for protection against mines, sabotage, or obstructed tracks. Passenger trains should carry a supply of ammunition and hand grenades for the crew and passengers to use if needed. They should also contain fire extinguishers and first-aid kits. All vestibule doors should be kept closed. This prevents guerrillas from boarding. Windows should be covered with securely fastened heavy mesh wire screen to prevent hand grenades or other explosives from being thrown into the cars. With security troops posted at strategic positions and trains carrying armed security forces, rail interruptions resulting from sabotage and guerrilla action can be greatly reduced.

c. Should the train be attacked, either by sniper fire or by ambush in force, the first consideration is to keep the train moving, if at all possible. The NCOIC of the security force should deploy his forces in the best manner to return fire and repel the attack. If the train is halted they should remain in the car if the security force car will withstand the fire of the attackers. If not, they should get off the train and take up the most advantageous firing positions. All possible fire should be directed to neutralize or destroy the attackers. They must, however, be familiar with and alert for the train whistle signal for reboarding, so they will not be left behind or injured trying to board the train as it moves out.

U-28 Air Attack

a. Trains, track, and all rail facilities are exceedingly vulnerable to air attacks. When trains are operated in areas subject to these attacks, antiaircraft weapons may be mounted on cars spaced throughout the train and manned by members of the security force attached to the battalion. When the train is attacked in open and exposed areas, it should continue to move if possible. Heavily wooded areas or deep cuts through banks or hills provide some cover. Trains attacked in such terrain should use whatever cover is available. Tunnels afford excellent cover for trains if the tunnels are long enough. Short tunnels can be used for hiding locomotives or cars containing special equipment.

b. If possible, trains operating in areas subject to air attack should run at night and stop in concealed places during the day. Diesel-electric locomotives can be camouflaged to look like boxcars. Steam locomotives are much more difficult to conceal. As a rule, rail lines are not considered profitable targets for airstrikes because they are quickly repaired. Rail installations such as terminals, port areas, and railheads generally suffer the greatest damage. Bridges and stations for refueling and watering locomotives are also likely targets. It is highly improbable that train operations could continue with any great degree of success under sustained air attacks.

U-29 Freight Security

The physical security or safekeeping of freight requires that all personnel are well trained in all phases of movement and protection of supplies. Because of the poor economic state that results from the ravages of war, pilferage and theft are continual threats in theaters of operations. Favorite targets of pilferers are food, clothing, fuel, tools, and other supplies that sustain life. This threat does not always come solely from local inhabitant. Freight must be protected against removal by any persons except those authorized to receive freight shipments. Usually, pilferage centers around small easy-to-carry items. Mail and high-priority materials always present security problems. The following paragraphs discuss some methods of achieving freight security at the origin of movement, while in transit, and at its destination.

U-30 Security at Origin

a. The shipper is responsible for the security of all carload freight until it is turned over to the TRS and the loaded car coupled to a locomotive for movement. Carload freight is that loaded by the carload, as opposed to a few boxes or crates of freight. The shipper is also responsible for properly loading the cars. This includes blocking and bracing, closing and sealing the car doors, icing if required, and documenting the cars. Before loading a car, he should inspect it thoroughly

to insure that it meets security requirements. Doors should be securely in place. No holes should be in the roof, sides, or floors. If he finds a defective car, he should report it immediately to the railway organization that supplied the car. It is very important that rail cars be loaded properly when they are turned over to the TRS for movement. The shipper's responsibility in getting them ready to move is discussed in detail in the following paragraphs.

b. One of the most vulnerable places during movement of cargo is the loading point. Rail cars should be loaded as soon as the freight is brought to the carrier. Loads should be evenly distributed over the car, so that no side or end is more heavily loaded than the other. Improper placement of the load can cause the car to sway and the load to shift. If shipments are made in open cars, they should be covered with securely fastened tarpaulins if the contents can be damaged by bad weather. If boxcars are available, small items should be shipped in them. CONEX containers are also ideal for shipping small items on flatcars. They reduce the turnaround time of the rail equipment, protect freight from weather, and greatly reduce the chance of pilferage.

c. The main objective of blocking and bracing is to insure that freight will be immobile during, transit and will arrive at its destination in good condition. Lumber used for blocking and bracing should be sound and free of knotholes and splits. These impair strength and interfere with nailing. Great emphasis should be placed on proper blocking and bracing of loads because of the danger of their shifting, and thereby breaking equipment and freight. Also, if a load shifts and a box or crate of small items breaks open, the chance of pilferage and theft is greatly increased. There are two very good reasons why this is true. It is much simpler to steal something that can be easily moved and hidden, and a thief is more likely to tamper with a broken crate or box. Second, most items are not identifiable from the outside of a box or crate. A thief will not usually go to a lot of trouble to steal something unless he knows that he can use it, sell it, or deprive US forces of critical material.

d. The standard method of sealing a railway car door (in addition to locks or wires) is by a soft metal strap or cable seal). Sealing the cars and containers may discourage pilferage but does not prevent it. Broken seals indicate that the car and contents have been tampered with just as unbroken seals normally indicate that the contents are secure. Train security forces or operating crews can easily check the seals on cars when the train stops and before it starts again. Any broken seals help pinpoint the time and place of the theft. It is important that a broken seal be reported immediately.

e. Rail cars and their loads are documented to aid in identifying and controlling them. When proper documentation is presented to TRS personnel, they are authorized to move the railway car. The document normally used in TRS operations is the Freight Waybill, or Government Bill of Lading (GBL). This form is filled in by the shipper or field transportation officer. It shows the car number, gives a brief description of its contents, weight of the load, names the consignor and consignee, and tells the origin and destination.In addition, it may show special instructions for the movement or security of the car and contents. One copy of this form accompanies the car. Each car has its own waybill rather than one large waybill for the entire train; because one or more cars maybe set out on a siding while en route if they become defective. An ade quate system of documentation is essential for the security of all rail shipments. Through the use of documents, it is easy to determine if something is missing from a shipment. They prevent the loss of a car or contents and provide a means of locating cars loaded with critical cargo so that priority movements can be authorized. Transportation movement officers are responsible for the completeness,

correctness, and proper handling of waybills. TRS is responsible for moving the freight and insuring that all instructions on shipping documents are followed. When the trip is completed, the secured cars are inspected by the receiver or his authorized agent. The NCOIC of the security force must obtain a receipt for those cars.

f. Insuring that cars containing perishable commodities are iced is the responsibility of the shipper. The TRS must insure that the car is routed so that any necessary re icing can be accomplished.

U-31 Security in Transit

a. In a theater of operations, when property and material are in transit, security problems are prevalent. Loading procedures, placing the cargo into carriers, and moving these carriers all present security hazards of varying degrees. Sabotage and pilferage may be encouraged because of the economic state or the political sympathy of the local population. All elements that contribute to security hazards must be evaluated to obtain the most effective security system possible. One way of insuring the security of cargo in transit is by having the responsibility of the consignor, the earner, and the consignee clearly established. In general, the protection of property and material in transit is there sponsibility of the person who has the ship ment in his custody. However, this varies according to its size and the means of transportation.

b. For shipments by rail, as stated in paragraph U-30a, the shipper is responsible for the security of loaded cars until they are prop erly turned over to the transportation railway service. TRS responsibility commences when the loaded and sealed cars are coupled to a locomotive or train. It ceases when the loaded cars are delivered to a designated depot siding, or track. The consignee or receiver assumes responsibility for the security of loaded cars at the time they are delivered at the designated depot, siding, or track.

c. Before moving a car from its loading origin, TRS personnel inspect it for defects, proper loading, secure seals, and proper documentation. The train operating crew and the train security forces are responsible for the security of the car and cargo. They must re port any discrepancies or interruption in the normal operating procedures during the entire movement. When operations permit, cars containing highly pilferable freight, high-priority cargo, or special shipments are grouped in the train to permit the most economical use of train security forces. If necessary, the shipper or loading agency also may assign specially trained personnel to safeguard critical or highly sensitive cargo in transit. Military police or other patrols should be stationed at critical portions of the route where attempts at pilferage may be expected. When cars containing such freight arrive in a rail yard, the yard-master makes note of the receipt of them. To expedite the shipment of sensitive cargo, information about the movement is normally transmitted from division to division by the chief train dispatcher through his telephone circuit. This method provides an efficient integration of high-priority shipments into the movements program.

d. The train security forces prepare and maintain a record by car number of all guarded cars in the train. They note and report any irregularities in procedures, the pre sence and actions of any unauthorized persons, and any deficiencies and/or incidents that occur en route. If these forces are relieved by other security forces while en route, an inspection of the guarded cars is made jointly by both crews, and the relief forces sign the record.

e. When the train is traveling at slow speeds on steep grades, through tunnels,

cuts, villages, or in wooded, restricted, or congested areas, the danger of looting or attack increases. Security forces and operating crews must be more alert for persons attempting to board or damage the train. When the train is stopped, security forces dismount and check the train on both sides. They verify that seals, locks, and wires are intact. They check for any damage to the cars, including overheating journal boxes, which may cause damage to the axles.

U-32 Security at Destination

a. Because unloading points are highly vulnerable to pilferage and sabotage, cars should be unloaded as soon as the train arrives at its destination. This may not always be possible; but immediate handling of freight reduces opportunities for its loss. Speedy unloading of rail cars also increases the availability of the rail equipment.

b. The wire sealing on closed car doors should be removed carefully to avoid breaking the door latches. After unloading, if the material must be stored, every possible effort must be made to achieve the desired level of security. Remember, both open and covered items in storage are vulnerable to all types of sabotage.

U-33 Trip Reports

At the conclusion of the trip, the NCOIC prepares a report covering the trip. There is no prescribed form, but the report should contain, in addition to the items listed in par. U-30d, the following:

• Dates and times of commencement and completion.

• Personal data of the security forces and train crews.

• Any recommendation for correction of deficiencies or improvement of duture train security operations.

Additional items may reincluded, either as required by local or command directives, or at the discretion of the NCOIC. The receipt ob tained for the secured cars (par. U-30e) must be attached to the report.

Pipeline Security — Section III

U-34 General

a. Pipeline (and hoseline) systems are used extensively, especially in active theaters of operations. They are used for economical delivery of large quantities of bulk petroleum products, especially automotive and aviation gasolines, diesel and jet fuels. They are generally designated as logistical or tactical pipeline systems. A **logistical system is either permanent or semipermanent. A tactical system is either temporary or semipermanent.** A tactical system consists of rapidly coupled pipe or tubing systems and rapidly emplaced storage tanks. It furnishes fuel to advancing units in corps or division areas. A variation of the tactical system is an assault pipeline system. This is composed of hose, collapsible fuel cells, and portable

pumps. It is rapidly installed to supply rapidly advancing troops in combat areas.

b. These systems consist, in general, of discharging facilities for tankers at ports, water terminals, or other points of entry; inland tank farms, terminals, and other storage and dispersing facilities; pump stations (which may be designated as trunk stations or booster stations when used on the main line, or as branch stations when used on a branch pipeline or hoseline); and pipelines that extend as far forward as practicable from the point of entry. Branch pipelines or hoselines are lines leading off the main pipe line to major users, such as airfields, or to general support suppliers.

c. Pipe and tubing used in the construction of military pipelines are of three main varieties—standard lightweight, standard weight, and special.

(1) Standard lightweight steel tubing makes up most of the length of the pipeline. This tubing comes in 20-foot sections. Lightweight tubing, because its wall is thin, is not normally buried nor used in submerged water course crossings. It also is not used in populated areas and other places where the hazards of fire and physical damage are great.

(2) Standard weight pipe is used where standard lightweight steel tubing does not give sufficient strength. Such pipe is used in submarine pipelines, river crossings, and other critical locations. Standard weight pipe may be either coupled or welded. In the Army it is usually coupled. It is fabricated in diameters of 4, 6, 8, 12, 16, 18, 20, and 22 inches. However, it is not normally stocked by the Army in diameters in excess of 12 inches.

(3) Special pipe and tubing includes pipe and tubing made of aluminum or other alloys or material. It is used where lightness of material is essential. Special tubing includes the flexible hoses used in the construction of beach manifolds. It also is used for unloading lines leading to offshore tanker anchorages. Hoselines also are used in forward areas, such as at pipeheads. They also may be used as temporary lateral extensions from rigid pipelines to supply points and airfields. Hoselines also can be used as temporary bypasses when sections of rigid pipeline are being repaired or replaced.

U-35 Security Hazards

a. Pipelines are vulnerable to a variety of security hazards throughout their lengths, from point of entry to point of final delivery.

b. Pilferage is the most common hazard, especially in areas where gasoline is scarce and expensive on the civilian market. Pipelines are tapped by loosening the flange bolts that join the sections of pipe. Gasoline draining through the opening is poured directly into containers of any type (depending on space available beneath the pipe) or permitted to fall into a hole dug under the line. From the hole it is transferred to containers. Much gasoline can be pilfered in this manner. Gasoline can be pilfered from hoselines by either loosening the couplings between sections of hose, or by cutting holes in the hoseline.

c. Such pilferage frequently causes fire or explosion along the pipeline. This is due to the spilling of highly volatile fuel during pilferage and afterward because flange bolts or hose couplings are seldom properly tightened. Also, the holes in hoselines are not plugged or mended.

d. Even when such actions of pilferers do not result in fire or explosion, they add immensely to the total loss because of the continued flow of petroleum from opened flanges or holes. Experience indicates that losses may exceed 16 percent over a 5-month

153-846 0 - 94 - 22

period from this type of activity in a theater of operations.

e. Sabotage is always a security hazard. It is committed by any method such as simply opening pipe flanges, cutting hoseline, or setting fires and causing explosions to destroy portions of a line.

f. Security hazards also exist at pumping stations, frequently at locations remote from supporting units. They are vulnerable to attack primarily for sabotage by destruction of either the pumping machinery or the entire station.

U-36 Organization and Planning for Security

a. Pipeline security may be performed either by military police units or by infantry units assigned to military police units, or both. Organization of forces and planning for security can be a responsibility of the military police commander. He must coordinate with the security officers of the pe troleum group and petroleum operating battalions. He must coordinate with other security officers, especially those with a physical security responsibility for any area through which the pipeline passes.

b. He should, where possible, coordinate with the pipeline construction and using agencies prior to construction. Here he can provide advice and recommendations on physical security. If the pipeline is already in operation, he should cause a thorough reconnaissance of the pipeline to be made from point of entry to terminal. He should include any branch lines, pumping stations, or other facilities.

c. The MP commander's coordination should include consultation with the command engineer. The engineer is responsible under the provisions of AR 415-22, for physical protection measures, including the hardening or dispersion of petroleum storage and related facilities. Types and methods of protection mentioned in that AR include

- Buried or semiburied construction
- Floating roof, suitably protected
- Splinter-proofing, blast walls, and revetments
- Use of natural terrain features
- Dispersion
- Use of security guards
- Other physical aids for protection against sa48botage.

The type and level of protection best suited and economically feasible for all elements of petroleum installations is determined by target analysis and feasibility evaluation. This is also an engineer responsibility. Protection from strafing, high explosive bomb ing, atomic blast, and fire must be considered. The AR contains a table that reflects the degrees of protection afforded by various means of construction against various types of attack. The physical security officer should be familiar with these procedures and cooperate with the engineer in his target analysis and feasibility evaluation.

d. The level of intensity of the warfare situation has a considerable effect on the type and extent of the security hazards to be anticipated. In a peacetime or stable situation, the chief hazard is usually pilferage. The extent of pilferage depends on the local availability and prices of petroleum products in the area. As the level of intensity increases from low to high intensity, the hazard of sabotage be comes increasingly important. Security measures should be increased and altered to meet this threat.

U-37 Security Considerations

a. One of the first security considerations is to coordinate all efforts, tactical and nontactical, in the area of the pipeline system to provide surveillance, report observations, and to take immediate actions to protect the system. Forces dedicated entirely to pipeline security are rarely sufficient in number for complete and continuous surveillance of the entire system. The security officer must deploy his forces in the best manner to provide coverage, by static, motorized, and air patrols, of the most vulnerable portions. Other portions must be covered by surveillance by other forces. These other forces in the course of their normal duties, can observe and report items of intelligence for further investigation. Some suspicious activities in the pipeline area might include the unusual presence of commercial tank trucks, appearance of gasoline drums or cans, or increased use of motor vehicles in fuel-scarce areas. These also include any unexplained personnel in the vicinity of the system, especially in remote places. All commanders must be impressed with the necessity for reporting such information, since the pipeline system represents such an important part of their subsistence.

b. A second consideration is the locations of terminals. These locations, as well as the size and number of terminals, depend on tactical, logistical, and similar military considerations. The principal military factor is the capability of an enemy to destroy one or more of the terminals. Another factor is the ability of other terminals to take over the functions of the terminals that may be destroyed. Such mandatory locations represent risks the commander must consider. The system represents a compromise between the requirements imposed by military necessity and the requirements for technical efficiency. The concern of the physical security officer is the defense of these terminals. It may be that he will have no voice in their selection; however, if he does, he should recommend those locations that lend themselves most suitably to static security. These may best serve as central control points for his static and roving patrols along the pipeline.

c. The pipeline itself should, insofar as possible, be laid in accordance with FM 10-67. Adherence to the following guidelines will, in addition to logistical considerations, provide the most beneficial situations from a security standpoint:

(1) The pipeline must follow the main military effort. In general, the route should take advantage of existing facilities and follow the most direct route feasible.

(2) The fundamentals of route selection are discussed in TM 10-1118 and TM 5-343. The latter also contains information pertaining to laying pipelines. Some of the more important considerations that in fluence route selection are listed next:

(a) Location, availability, and condition of pier or wharf facilities.

(b) Geographic and topographic considerations in establishing tanker unload ing and base terminal facilities.

(c) Location, availability, and condition of existing military or civilian pipe lines and petroleum products tankage.

(d) Probable need for dispersal of facilities.

(e) Planned or actual location of major fuel-consuming installations, such as naval supply depots and airfields. Pipe lines used chiefly to supply bulk aviation fuels generally follow the most direct route to the airbases, with branch lines as required. Hoselines may be used when necessary as expedient branch lines. Responsibility of the Army ends with the delivery of the product to the Navy or Air Force base perimeter.

(f) Use of secondary all-weather roads to support construction of the pipelines

and to facilitate their securit y, supply, and maintenance.

(g) Maximum use of cover and concealment consistent with other criteria.

(h) Avoidance of such natural obstacles and barriers as swamps and rivers. Avoidance of urban and industial areas and other potential profitable targets. Pipelines should not parallel opcrating railroads; neither should they be laid near railroads used by coal-burning locomotives, unless there is no other place to locate them.

(i) Compatibility, as required and feasible, with post-hostilities requirements and plans.

d. Pump stations are vital elements in the pipeline system. Not only do they push the products through the pipeline, they also feed the pipeline and may be used to transfer fuel between tanks and supply dispensing outlets. The location and spacing of pump stations depends upon the hydraulic design of the pipeline and the topographic features of the pipeline route. Location and spacing also depend upon the type and properties of the fuel to be pumped, operating characteristics of the pumping units selected, and the friction head losses for the selected size of pipe. In addition, spacing of stations must take into account effective control and maintenance of the line and efficient administration of the troop units that build and operate it. Underground shelter should be provided, when practicable, to protect personnel against attack.

e. An important consideration for security is the question of whether the pipeline should or should not be buried. Also to be considered is whether tanks should be buried, or covered with earth or other protective covering. (Note: Standard lightweight steel tubing is not normally buried. Standard weight pipe is required for burying.) The advantage of burying pipe and tanks is greater security, concealment from aerial observation, and reduced maintenance requirements. The physical security officer should stress these advantages and recommend burial when practicable. As an alternative, all possible means of cover and camouflage must be recommended. If burial is accomplished, it should be at a depth sufficient for protection against small arms fire or fire from any aircraft called in for spraying (par f, next). It should also protect the pipe and tanks from aircraft or mortar flares falling to the ground before burnout.

f. The physical security officer should coordinate with appropriate agencies for air surveillance of pipeline systems. He should arrange for helibome night illumination when required. He should arrange for airstrikes on call to “spray” particular portions of the system area when essential to drive off saboteurs. Plans for such actions must be carefully made to preclude damage to the system or injury to friendly forces or innocent civilians.

g. Arms and equipment for security forces vary according to the tactical level of intensity, the prevailing situation, opposition anticipated or experienced, and similar factors. Radio communications are essential, and should be tied in with all available supporting forces in the area.

h. Finally, the physical security officer must be aware and alert for changes in the type and density of the population in areas adjacent to pipeline systems. The need for civic action requires coordination with appropriate military and civilian authorities for the education of local populations in the importance of the pipeline to their welfare. It should address the dangers to them if they interfere with its operation. This is particularly important when rapid population growth is observed, such as the springing up of new refugee hamlets or villages in the vicinity. The reasons for such growth must be analyzed. Any indication that it is connected with access to the pipeline for pilferage or other such activities should be investigated thoroughly.

Order of Economy	Most Effective Use	Capabilities	Limitations
Motor transport	Supplementary mode for providing the connecting link for an integrated transportation system. It can also be used effectively in scheduled line haul operations by the trailer relay system. Primary mode for distribution operations and for logistical support operations in the combat zone.	Most flexible mode over trafficable terrain; practically all weather (terrain factor important); increases flexibility of other modes; can transport nearly any commodity with a variety of specialized equipment for both on- and off-road movement.	Over-the-road operations influenced by route interferences and by obstacles created by weather, terrain, or enemy action; sustained line haul operations over long distances uneconomical in terms of ton-mile output versus expenditure of manpower and equipment.
Rail	Primary inland mode for maintaining a sustained flow of large quantities of traffic over long distances.	All-weather; any commodity; most economical continuous line haul operation; greatest sustained ton-mile capability; a variety of specialized equipment and services.	Flexibility limited by fixed routes; rail line clearances restrict outsize movements; capability limited by availability of motive power; rail line highly vulnerable to enemy action.
Water	Primary over-ocean mode. Supplementary inland surface mode for movement of large quantities of cargo in bulk and heavy and outsize materiel.	All-weather; any commodity; most economical overall long-distance carrier; particularly useful for relieving other modes for more suitable employment.	Relatively slow; flexibility limited by adequacy of terminals, waterways facilities, and channels; vulnerable to enemy action and difficult to restore.
Air	Complementary mode for providing expedited movement of mission-essential traffic. Primary or major supplementary mode when terrain conditions reduce effectiveness of surface modes. Scheduled operation is the most economical method of employment and produces greatest sustained ton-mile capability.	Greatest potential speed of delivery and most flexible with respect to terrain obstacles. When these factors are combined with substantial lift capability, air transport over long distances becomes more economically favorable.	Operational capabilities and effectiveness limited by weather factors and trafficability of takeoff and landing areas. Relatively high ton-mile operating costs.
Pipeline	Primary mode for bulk liquids and solids suspended in liquid.	All-weather; few terrain restrictions; most economical and reliable mode for bulk liquids; relatively few personnel required for operation and maintenance.	Flexibility limited by immobile facilities; vulnerable to sabotage and enemy action; large construction tonnages required.

Figure II-1 Mode selection guide

Class I—Subsistence.

Class II—Clothing, individual equipment, tentage, organizational tool sets and toolkits, handtools, administrative, and housekeeping supplies and equipment.

Class III—POL: Petroleum fuels, lubricants, hydraulic and insulating oils, preservatives, liquid and compressed gases, bulk chemical products, coolants, deicing and antifreeze compounds, together with components and additives of such products, and coal.

Class IV—Construction materials to include installed equipment and all fortification/barrier materials.

Class V—Ammunition of all types (including chemical, biological, radiological, and special weapons), bombs, explosives, mines, fuses, detonators, pyrotechnics, missiles, rockets, propellants, and other associated items.

Class VI—Personal demand items (nonmilitary sales items).

Class VII—Major End Items: A final combination of end products which is ready for its intended use, such as, launchers, tanks, mobile machine shops, and vehicles.

Class VIII—Medical materiel, including medical-peculiar repair parts.

Class IX—Repair Parts (less medical—peculiar repair parts): All repair parts and components to include kits, assemblies, and subassemblies, reparable and nonreparable, required for maintenance support of all equipment.

Class X—Materiel to support nonmilitary programs, such as, agricultural and economic development, not included in classes I through IX.

Figure U-2. Classes of supply.

Appendix V

References

Army Regulations (ARs)

1-4	Employment of Department of Army Resources in Support of the United States Secret Service
10-5	Department of the Army
10-6	Branches of the Army
10-23	United States Army Criminal Investigation Command
18-7	Data Processing Installation Management, Procedures, and Standards
20-1	Inspector General Activities and Procedures
20-3	Superseded by AR 190-53, Interception of Wire and Oral Communications for Law Enforcement Purposes.
27-40	Litigation
36-75	Audit Procedures for Nonappropriated, Trusts, and Other Official Funds Other Than Army Club Systems
37-103	Finance and Accounting for Installations; Disbursing Operations
40-2	Army Medical Treatment Facilities General Administration
40-3	Medical, Dental, and Veterinary Care
40-61	Medical Logistics Policies and Procedures
40-202	Assignment and Utilization of Army Medical Department Personnel
50-5	Nuclear Surety
50-6	Chemical Surety Program
55-16	Movement of Cargo by Air and Surface-Including Less Than Release Unit and Parcel Post Shipments
55-29	Military Convoy Operations in CONUS

55-38 Reporting of Transportation Discrepancies in Shipments
55-55 Transportation of Radioactive and Fissile Materials Other Than Weapons
55-162 Permits for Oversize, Overweight, or Other Special Military Movements on Public Highways in the United States
55-203 Movement of Nuclear Weapons, Nuclear Components, and Related Classified Nonnuclear Materiel
55-228 Transportation by Water of Explosives and Hazardous Cargo
55-355 Military Traffic Management Regulation
59-11 Army Use of Logistics Airlift (LOGAIR)
70-1 Army Research Development and Acquisition
95-27 Operational Procedures for Aircraft Carrying Dangerous Materials
190-5 Motor Vehicle Traffic Supervision
190-10 Security of Government Officials
190-11 Physical security of Weapons, Ammunition, and Explosives
190-12 Military Police Working Dogs
190-13 The Army Physical Security Program
190-14 Carrying of Firearms
190-18 Physical Security of US Army Museums
190-21 Security Identification Credentials and Application
190-22 Search, Seizure and Disposition of Property
190-28 Use of Force by Personnel Engaged in Law Enforcement and Security Duties
190-40 Serious Incident Report
190-45 Records and Forms
190-49 Physical Security of Arms, Ammunition, and Explosives In-Transit
190-50 Physical Security for Storage of Controlled Medical Substances and Other Medically Sensitive Items
190-53 Interception of Wire and Oral Communications for Law Enforcement Purposes.
195-2 Criminal Investigation Activities
210-10 Administration
220-5 Designation, Classification, and Change in Status of Units
220-58 Organization and Training for Chemical, Biological, and Radiological Defense Operations
230-1 The Nonappropriated Fund System
230-6 Amusement Machines
230-7 Auditing Services and Audit Compliance for Open Messes, Revenue—Producing Funds, and Other Sundry Funds
230-9 Internal Controls
230-65 Nonappropriated Funds Accounting Procedures for Revenue Producing Sundry and Welfare Funds
310-1 Publications, Blank Forms, and Printing Management
310-25 Dictionary of United States Army Terms
310-31 Management System for Tables of Organization and Equipment (The TOE System)

310-49 The Army Authorization Documents System (TAADS)
310-50 Authorized Abbreviations and Brevity Codes
340-1 Records Management Program
340-3 Official Mail
340-16 Safeguarding for "Official Use Only" Information
350-4 Qualification and Familiarization With Weapons and Weapons Systems
360-5 Public Information Policies
380-5 Department of the Army Supplement to DOD 5200.1-R
380-20 Restricted Areas
380-25 Foreign Visitors
380-55 Safeguarding Defense Information in the Movement of Persons and Things
385-40 Accident Reporting and Records
385-55 Prevention of Motor Vehicle Accidents
385-63 Regulations for Firing Ammunition for Training, Target Practice, and Combat
385-80 Nuclear Reactor Health and Safety Program
405-20 Federal Legislative Jurisdiction
405-25 Annexation
420-70 Buildings and Structures
420-90 Fire Prevention and Protection
500-50 Civil Disturbances
500-60 Disaster Relief
500-70 Military Support of Civil Defense
570-2 Organization and Equipment Authorization Tables-Personnel
570-4 Manpower Management
600-40 Apprehension, Restraint, and Release to Civil Authorities
604-5 Clearance of Personnel for Access to Classified Defense Information and Material
606-5 Personnel Identification: Identification Cards, Tags, and Badges
614-3 Assignment of Military Personnel to Presidential Support Activities
670-5 Male Personnel
670-10 Furnishing Uniforms or Paying Uniform Allowances to Civilian Employees
(0)700-65 Nuclear Weapons and Nuclear Weapons Materiel
710-2 Materiel Management for Using Units, Support Units, and Installations
740-7 Safeguarding of Sensitive, Drug Abuse Control, and Pilferable DSA Items of Supply

DA Pamphlets

27-21 Military Administrative Law Handbook
570-4 Manpower Procedures Handbook

Field Manuals (FMs)

3-8	Chemical Reference Handbook
3-12	Operational Aspects of Radiological Defense
3-15	Nuclear Accident Contamination Control
3-21	Chemical-Biological Contamination and Control
5-15	Field Fortification
7-10	The Rifle Company, Platoon and Squads
9-6	Ammunition Service in the Theater of Operations
9-38	Conventional Ammunition Unit Operations
9-47	Special Ammunition Unit Operations
19-1	Military Police Support, Army Divisions and Separate Brigades
19-4	Military Police Support, Theater of Operations
19-5	The Military Police Handbook
19-15	Civil Disturbances
19-20	Law Enforcement Investigations
19-25	Military Police Traffic Operations
19-35	Military Police Working Dogs
20-20	Basic Care and Training of Military Dogs
20-32	Mine Countermine Operations at the Company Level
21-6	How to Prepare and Conduct Military Training
21-11	First Aid for Soldiers
21-15	Care and Use of Individual Clothing and Equipment
21-40	Nuclear, Biological, and Chemical (NBC) Defense
21-41	Individual Defense (NBC)
21-48	Planning and Conducting Chemical, Biological, Radiological; (CBR), and Nuclear Defense Training
21-150	Combative
22-5	Drill and Ceremonies
22-6	Guard Duty
22-100	Military Leadership
23-9	M16A1 Rifle and Rifle Marksmanship
23-35	Pistols and Revolvers
30-15	Intelligence Interrogation
31-36 (Test)	Night Operations
31-50	Combat in a Fortified and Builtup Area
31-85	Rear Area Protection (RAP) Operations
55-17	Terminal Operations Specialist Handbook
55-30	Army Motor Transport Operations
55-70	Army Transportation Container Operations
101-5	Staff Officers Field Manual, Staff Organization and Procedure

Training Circulars (TCs)

7-1	The Rifle Squad (Mechanized and Light Infantry) (How to Fight)
7-3	The Rifle Platoon

Technical Manuals (TMs)

3-220	Chemical, Biological, and Radiological (CBR) Decontamination
5-225	Radiological and Disaster Recovery at Fixed Military Installations
5-315	Firefighting and Rescue Procedures in Theaters of Operations
5-805-8	Building Construction Materials and Practices: Builder's Hardware
5-820-4	Drainage and Erosion Control: Drainage for Areas Other Than Airfields
5-830-3	Planting: Dust Control
5-6350-262 -Series	Appropriate to Installed Joint-Service Interior Intrusion Devices System
9-1300-214	Military Explosives
9-Series	Appropriate to Assigned Weapons
11-Series	Appropriate to Assigned Communications Equipment
21-300	Driver Selection and Training (Wheeled Vehicles)
55-311	Motor Convoy Security in Stability Operations
55-312	Military Convoy Operations in CONUS
55-602	Movement of Special Freight

Technical Bulletins

MED 291	Guidance for Inventory, Control, and Accountability of Drugs and Injection Devices of Potential Abuse at Medical Treatment Facilities Worldwide
5-6350-262	Selection and Application of Joint-Service Interior Intrusion Devices System

DOD Regulations and Manuals

4160.21-M	Defense Disposal Manual
4500.32-R	Vol I - Military Standard Transportation and Movement Procedures
4500.32-R	Vol II - Military Standard Transportation and Movement Procedures-Transportation Account Codes (TACS)
5200.1-R	(DOD) Information Security Program Regulation
5200.28-M	Manual of Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating-Secure Resource-Sharing ADP Systems

Army Training and Evaluation Program (ARTEP)

19-97	Military Police Physical Security Company

Tables of Organization and Equipment (TOE)

19-97G	Military Police Physical Security Company
19-97H4	Military Police Physical Security Company

Miscellaneous

9 (MCM)	Manual for Courts-Martial, United States, 1969 (Revised)

International Standardization Agreements (STANAG) and Standard of Operations and Logistics Agreements (SOLOG)

2041	Operational Road Movement Orders, Tables, and Graphs (SOLOG No. 51)
2042	Method of Challenging by Guards and Sentries
2047	Emergency Alarms of Hazard or Attack (SOLOG No. 110)
2079	Rear Area Security and Rear Area Damage Control
2154	Definitions and Regulations for Military Motor Movements by Road
2155	Road Movements and Transport Documents
2158	Identification of Military Trains

Preface

Introduction

This field manual sets forth guidance for all people responsible for physical security. It's the basic reference for training security personnel. It also covers requesting additional equipment and manpower.

The two primary concerns of this manual are prevention and protection. Both serve the security interest of people, equipment, and property. To be most effective, this interest must be supported at all staff and command levels. This support must be unified.

Physical Security Responsibilities

Major responsibilities in physical security exist at Department of the Army (DA) through local command levels (AR 190-13). These are as follows:

- Law Enforcement Division, Deputy Chief of Staff for Personnel—DA policy and procedures, Army-wide guidance, assistance, and development of physical security equipment.
- Assistant Chief of Staff for Intelligence—assessment of counterintelligence in physical security plans and programs.
- Chief of Engineers—final technical review and approval of plans and specifications for installing intrusion detection systems estimated to cost more than $5,000.
- Local Commanders—all reasonable precautions are taken to safeguard the people and property of their commands. Each commander must designate a physical security manager to plan, formulate, and coordinate physical security matters (AR 190-13). In short, the physical security manager formulates the plan; supervises physical security inspections, coordinates required support

(personnel and equipment); and reviews all plans for new construction or modification to insure all possible physical security safeguards are built in, and deficiencies eliminated or minimized. Normally, he is also responsible for physical security education programs for all personnel (chapter 3).

Arrangement of This Manual

You will find the arrangement, of this manual different from that of the previous FM 19-30. It should make physical security easier to understand and easier to apply. There is a brief introduction to each major area; and critical points are highlighted throughout for rapid review or scanning for important items. The guidance permits you the flexibility so critical to effective application (based on location, size of installation, etc.). There are also new checklists for standard security operations in CONUS and overseas.

How To Use It

This manual is to be used with the policy, doctrine, and training set forth in those references listed in appendix V.

Considerations

Perfect or absolute security is always our goal. However, a state of absolute security can never be attained. There is no object so well protected that it cannot be stolen, damaged, destroyed, or observed by unfriendly eyes. The purpose, then, of physical security is to make access so difficult that an intruder will hesitate to attempt penetration, or to provide for his apprehension should he be successful. Security must be built upon a system of defense in depth or upon accumulated delay time.

Physical security is only part of the overall defense of an installation. Defense against direct enemy attack and natural disasters must be blended into a system that includes physical security. This blended effort begins with planning.

It is not economically possible or theoretically necessary for installations and activities of every kind and character to achieve the same degree of protection. How much protection is warranted in any particular case depends on certain factors. If the installation is highly critical and highly vulnerable, an extensive physical security program is necessary.

All military installations are valuable in some degree to the national defense structure. Some are more valuable than others. To determine the degree of importance, the effect of partial or complete loss must be calculated. If the influence on the national defense effort is great, then criticality y is high. Within each installation, certain facilities are essential to the mission of that installation. Facilities such as primary and auxiliary power sources are highly critical.

Because of the monetary and manpower costs of physical protection, many commanders will not be able to achieve maximum protection for the entire installation or activity. Therefore, the specific criticality and vulnerability of various areas must be determined, and available resources divided accordingly. Special protection is thus provided for the most critical and vulnerable areas, while areas of less importance and susceptibility are given less protection.

A highly critical area is one in which partial or complete loss would have an immediate and serious impact on the ability of an installation or activity to perform its mission for a considerable time. The relative criticality of such an area may have no direct relationship to its size or whether it produces an end product. This must be determined upon the basis of its importance to the

installation or activity as a whole.

Vulnerability depends on the hazards that could cause sufficient loss, damage, or destruction to influence operation of the activity or installation. If one or more hazards exist that could easily achieve this result, relative vulnerability is high. As it becomes more unlikely that existing hazards will interfere with the mission, vulnerability becomes lower.

Applicability

All of the general considerations previously discussed are equally applicable to units and other operations. They are applicable to port and harbor security; to docks and wharves; to security escort operations; to POL distribution methods, including pipelines; to postal, finance, and many other operations. They are, in greater or lesser measure and with any necessary modifications, applicable to virtually any physical security situation.

This manual contains doctrine applicable to the security manager and to the guard. There is no need for the guard to know the procedures needed to obtain personnel and equipment. However, the manager—and to a lesser degree, the supervisor—must have this knowledge at his disposal to properly support and train all security personnel.

The techniques described in the following chapters can be readily adapted to a host of systems to be secured. But remember, physical safeguards, like tactical barriers for defense, require the backing of a trained and alert (security) force. Also, there must be proper execution of administrative/operational checks and procedural safeguards.

Index

153-846 0 - 94 - 23